

**ИНСТИТУТ ПРОБЛЕМ РЕГИСТРАЦИИ ИНФОРМАЦИИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК УКРАИНЫ**

На правах рукописи

ХИЦКО ЯНА ВЛАДИМИРОВНА

УДК 004.94

**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАДАЧ
КРИПТОГРАФИИ И ОБРАБОТКИ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ
НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ**

Специальность 01.05.02 – Математическое моделирование и
вычислительные методы

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:

доктор технических наук, профессор

Синьков Михаил Викторович

доктор технических наук, с.н.с.

Калиновский Яков Александрович

Киев – 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
РАЗДЕЛ 1. АНАЛИЗ ФОРМ ПРЕДСТАВЛЕНИЯ ДАННЫХ В МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ	15
1.1. Формы представления информации в математическом моделировании и их применения	15
1.2. Гиперкомплексная форма представления информации; неканонические гиперкомплексные числовые системы.....	21
1.3. Методы построения алгебраических характеристик гиперкомплексных числовых систем.....	27
1.4. Анализ существующих моделей задач криптографии и обработки сигналов с представлением информации в гиперкомплексных числовых системах и постановка задачи дальнейших исследований.....	35
Выводы по разделу 1.....	37
РАЗДЕЛ 2. РАЗВИТИЕ ТЕОРЕТИЧЕСКИХ ОСНОВ СИНТЕЗА И АНАЛИЗА НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ.....	38
2.1. Разработка общего алгоритма перечисления неканонических гиперкомплексных числовых систем.....	38
2.2. Перечисление неканонических гиперкомплексных числовых систем изоморфных диагональным системам	41
2.3. Исследование некоторых классов изоморфизма неканонических гиперкомплексных числовых систем размерности 2	48
2.4. Переход от бесконечномерной ГЧС к конечномерным ГЧС методами факторизации	52
2.5. Метод синтеза конечномерных ГЧС путем факторизации бесконечномерной ГЧС с двухточечным представлением элементов	57
2.6. Основные операции в неканонических ГЧС.....	63

2.7. Использование изоморфизма неканонических ГЧС для повышения эффективности операций.....	65
Выводы к разделу 2.....	68
РАЗДЕЛ 3. СВОЙСТВА НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ И ОПЕРАЦИИ В НИХ.....	70
3.1. Исследование алгебраических свойств неканонических гиперкомплексных числовых систем.....	70
3.2. Модулярная арифметика в неканонических гиперкомплексных числовых системах.....	82
3.3. Процедура, реализующая алгоритм Евклида для неканонических гиперкомплексных числовых системах.....	87
Выводы по разделу 3.....	93
РАЗДЕЛ 4. РЕШЕНИЕ ПРАКТИЧЕСКИХ ЗАДАЧ С ПРИМЕНЕНИЕМ НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ.....	95
4.1. Математическое моделирование задачи разделения секрета с использованием неканонических гиперкомплексных числовых систем.....	95
4.2. Синтез структур цифровых фильтров с оптимизированной чувствительностью в неканонических гиперкомплексных числовых системах.....	116
Выводы по разделу 4.....	139
ВЫВОДЫ.....	141
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	144
Приложение А. Справка про использование результатов диссертационной работы.....	157
Приложение Б. Структура программно-аналитического инструментария в пакете MAPLE.....	158
Приложение В. Листинги кода программно-аналитического инструментария в пакете MAPLE.....	159
Приложение Г. Неканонические ГЧС, изоморфные комплексным числам.....	168

ВВЕДЕНИЕ

Актуальность темы. Расширение круга задач в науке и технике требует развития и совершенствования методов математического моделирования, одним из важных компонентов которого является форма представления информации и обработки данных.

Выбор формы представления данных оказывает существенное влияние на быстродействие алгоритмов. В свою очередь, вопрос быстродействия алгоритмов, работающих с большими объемами данных актуален и теперь. Для больших объемов информации, как правило, используют структурные формы представления массивов данных, которые, в свою очередь, для представления каждого элемента такого массива, могут использовать любую форму. Существуют такие структурные формы представления данных как: векторно-матричная, полиномиальная, системы остаточных классов, а также гиперкомплексная [1-3].

Переход от вещественных параметров моделей к различным гиперкомплексным числовым системам является одним из методов повышения эффективности алгоритмов математического моделирования. В настоящее время можно сформулировать некоторые частные методы перехода в гиперкомплексные области:

- применение таких гиперкомплексных числовых систем (ГЧС), в которых компоненты гиперкомплексных переменных будут представлять собой параметры моделей или функции от них, операции с такими гиперкомплексными числами будут соответствовать операциям над параметрами модели в процессе моделирования;

- представления параметра модели в виде гиперкомплексных чисел таким образом, что законы функционирования модели примут достаточно простой вид;

- объединение последовательностей значений параметров модели в одно многомерное гиперкомплексное число таким образом, чтобы обработка

последовательности значений была сведена к более эффективным операциям над гиперкомплексным числом [4].

Методы представления и обработки данных в гиперкомплексных числовых системах (ГЧС) дают преимущества, которые позволяют значительно повысить эффективность моделирования задач электротехники, аэродинамики, навигации, квантовой механики, теории колебаний, криптографии, обработки сигналов и многих других.

География работ теоретического и практического направлений по исследованию гиперкомплексных форм представления данных включает США, Великобританию, Германию, Россию, Францию, Японию, Румынию и многие другие страны [5-17]. Среди исследователей, которые развивали методы ГЧС на ранних этапах, необходимо выделить таких выдающихся ученых как: Л.Эйлер, В. Гамильтон, О. Коши, Г. Грассман, Г. Вессель, Э.Штуди, И.М.Виноградов, А.Кэли, К.Вейерштрасс, Б.Пирс, В.Клиффорд, Ф.Молин, Г.Фробениус, Р.С.Болл, Э.Нетер [18-22]. В дальнейшем значительный вклад в развитие методов ГЧС в теоретическом плане сделали: А. Курош, Ю.М. Березанский, Ю.А. Дрозд, А.А. Бухштаб, Б.А. Розенфельд, В.В. Люш [23], Н.Г. Чеботарев. В частности В.В. Люш [23] представил исследования по неканонической гиперкомплексной числовой системе триплексных чисел, которая на сегодня является, по сути, единственной хорошо изученной неканонической ГЧС. В научно-практическом направлении исследования числовых систем сделали свой вклад И.Л.Кантор, А.С.Солодовников, В.Н.Бранец, И.П.Шмыглевский, И.Я.Акушский, А.А. Калюжный, И.П. Мельниченко, В.М.Чернов, К.Г.Самофалов, В.Ф.Евдокимов, М.В.Синьков, Н.В.Кошляков, В.Ф. Евдокимов, В.П.Тарасенко, Г.М.Луцкий, Я.А.Калиновский, Ю.А.Курочкин, Н.М.Губарени, Ш. Тойошима, Ю.Е. Бояринова и другие [24-26].

Отдельно хотелось бы выделить работы научной школы, созданной профессором М.В. Синьковым в Институте проблем регистрации информации НАН Украины. Основными направлениями деятельности этой школы на

протяжении последнего десятилетия являются исследования использования гиперкомплексных числовых систем как формы представления данных в таких областях, как криптография, а именно схемы разделения секрета (работы М.В. Синькова, Ю.Е. Бояриновой), синтез цифровых фильтров и создание алгоритмов выполнения свертки с помощью ГЧС (работы Я.А. Калиновского, А.В. Федоренко) и другие [25-37].

При моделировании задач вышеуказанных направлений, в основном, исследовались канонические гиперкомплексные числовые системы. Например, применение канонических ГЧС в задаче разделения секрета позволило значительно улучшить криптостойкость алгоритма (оценка криптостойкости зависит от размерности и вида числовой системы) [34]. Однако следует отметить, что увеличение криптостойкости задачи разделения секрета напрямую связано с увеличением размерности гиперкомплексной числовой системы, что увеличивает количество элементарных операций при реализации данной модели. Поэтому актуальным является представление исходных данных в неканонических ГЧС и модификация модели разделения секрета, что может позволить увеличить криптостойкость алгоритма без наращивания размерности такой системы.

Известны работы по эквивалентированию цифровых фильтров с вещественными коэффициентами цифровыми фильтрами с гиперкомплексными коэффициентами. Предложенные модели рекурсивных фильтров с гиперкомплексными коэффициентами в канонических ГЧС позволяют снизить суммарную параметрическую чувствительность фильтров до 20% [35-37]. Но поскольку количество систем, применимых для таких моделей, ограничено, эквивалентирование цифрового фильтра с представлением коэффициентов в неканонических ГЧС дает широкие возможности для дальнейшей оптимизации фильтра по параметрической чувствительности.

Кроме практического применения, исследование неканонических ГЧС может иметь большое значение для решения теоретических задач, таких как

перечисление классов изоморфизма, построение алгебраических характеристик и исследование модулярных операций.

Все вышеуказанное обуславливает актуальность избранного направления работ и перспективность теоретических и практических исследований в области неканонических ГЧС, что объясняет выбор темы диссертационной работы.

Связь работы с научными программами, планами, темами. Диссертационная работа выполнялась в рамках работ, проводимых в Институте проблем регистрации информации НАН Украины. К таким работам относятся:

- проект Государственного фонда фундаментальных исследований УКРАИНА-БЕЛОРУСЬ “ДФФД-БРФФД-2005” №Ф10/18-2005 “Исследования и использование гиперкомплексных числовых систем в задачах динамики, кинематики и кодирования информации” (регистрационный номер 0105U008393), 2005-2006гг.;
- научно-исследовательская тематика “Куб-1” - “Развитие теоретических положений многомерных систем данных и их использование для решения практических задач” (регистрационный номер 0104U003174), 2004-06гг.;
- научно-исследовательская тема “Куб2” – “Развитие методов представления и обработки многомерных данных для решения задач защиты информации, цифровой фильтрации и реструктуризации томографических изображений” (регистрационный номер 0107U002395), 2007г.

Целью исследований является повышение эффективности математических моделей задач криптографии и обработки сигналов путем разработки методов и способов представления данных в неканонических гиперкомплексных числовых системах.

Задачи исследований.

1. Проанализировать и модифицировать методы построения структур и классов изоморфизма неканонических ГЧС.

2. Усовершенствовать и разработать методы определения основных алгебраических характеристик и выполнения линейных, нелинейных и модулярных операций в неканонических ГЧС различной размерности, а также программно-алгоритмические средства их реализации.
3. Разработать и реализовать модификацию математической модели криптографической задачи разделения секрета с помощью представления данных в неканонических гиперкомплексных числах. Провести анализ эффективности такой модели.
4. Разработать метод синтеза цифровых фильтров с гиперкомплексными коэффициентами в неканонических ГЧС.
5. Разработать и реализовать методы оптимизации параметрической чувствительности фильтра, представленного с помощью неканонических ГЧС.

Объектом исследования являются процессы моделирования задач криптографии и обработки сигналов с помощью представления данных в неканонических гиперкомплексных числовых системах.

Предметом исследования являются модели задач разделения секрета и оптимизации суммарной параметрической чувствительности цифрового фильтра и методы их решения.

Методы исследования. Для достижения цели исследования используются общая алгебра, теории чисел, гиперкомплексных числовых систем, цифровой обработки сигналов и криптографии; методы решения систем сравнений; экспериментальные исследования эффективности предложенных моделей, методов, алгоритмов.

Научная новизна полученных результатов. В процессе решения поставленных задач получены такие научные результаты:

1. Усовершенствованы методы построения структур гиперкомплексных числовых систем заданной размерности, которые отличаются от существующих тем, что структурно устанавливают заданные

ограничения области представления данных в неканонических ГЧС, что приводит к снижению количества операций при построении таких структур и расширяет возможности их использования в практических задачах.

2. Получили дальнейшее развитие методы определения основных характеристик неканонических ГЧС и выполнения операций в них, в том числе метод вычисления вычетов в неканонических ГЧС, которые, в отличие от существующих методов, учитывают структурные особенности неканонических ГЧС заданной размерности, что дало возможность повысить эффективность моделирования практических задач с представлением данных в неканонических ГЧС.
3. Модифицирована математическая модель схемы разделения секрета, которая отличается от существующей представлением информации остатками в неканонических ГЧС по совокупности неканонических гиперкомплексных модулей, что дает возможность уменьшить количество вычислений при обеспечении такой же криптостойкости по сравнению с такой же моделью, которая использует канонические ГЧС.
4. Впервые предложен метод синтеза множества неканонических ГЧС, удовлетворяющих критериям построения цифрового фильтра с неканоническими гиперкомплексными коэффициентами, который дал возможность решить задачу оптимизации цифрового фильтра.
5. Впервые предложен метод оптимизации суммарной параметрической чувствительности фильтра с гиперкомплексными коэффициентами в неканонических ГЧС, использующий поиск локального минимума для заданного диапазона значений параметров модели и позволяющий существенно уменьшить параметрическую чувствительность эквивалентного фильтра с вещественными коэффициентами.

Практическое значение полученных результатов.

1. Создан аналитически-программный инструментарий, который реализует предложенные модели и средства, и позволяет решать прикладные задачи с представлением данных в неканонических ГЧС, в том числе, задачу моделирования схемы разделения секрета и синтеза цифрового фильтра с гиперкомплексными коэффициентами, а также решать задачу оптимизации чувствительности цифрового фильтра с гиперкомплексными коэффициентами в неканонических ГЧС. Реализованные в инструментарии методы построения структур неканонических ГЧС заданной размерности и с заданными ограничениями позволяют получить множество таких систем для представления данных в них.
2. Полученные результаты математического моделирования задачи разделения секрета в неканонических ГЧС могут быть использованы как часть автоматизированной системы защиты информации, в частности, в протоколах тайного голосования.
3. Полученные научные результаты работы относительно синтеза рекурсивного цифрового фильтра с гиперкомплексными коэффициентами в неканонических ГЧС и метод его оптимизации по параметрической чувствительности использованы в работе программного обеспечения, внедренного на ДП Научно-производственный комплекс “Прогресс” для координато измерительной машины CONTURA G2.

Личный вклад заключается в теоретическом обосновании полученных результатов, которые проверены на большом количестве примеров. Все научные результаты диссертации получены автором самостоятельно.

В работах, опубликованных в соавторстве, соискателю принадлежит:

[4] – структура и функции алгоритмически-программной системы вычислений в неканонических ГЧС в среде MAPLE;

[60] – исследование алгоритма Евклида при представлении данных гиперкомплексными числами;

[61-62] – программная реализация алгоритма Евклида для восстановления информации в задаче разделения секрета с использованием ГЧС;

[63-64] – сравнительные характеристики применения ГЧС и вещественных чисел в алгоритмах RSA;

[98-99] – исследование классов изоморфизма неканонических ГЧС размерности 2 к системе прямой суммы вещественных чисел;

[101-102] – примеры систем, полученных по результатам факторизации бесконечномерной ГЧС;

[103-105] – анализ сложности вычислительных процедур в системе антикватернионов;

[109] – вычислительные процедуры для неканонических ГЧС и таблицы сопоставления сложностей вычислительных процедур для неканонических и канонических ГЧС;

[112-113] – предложен метод оптимизации суммарной параметрической чувствительности цифровых фильтров.

Апробация результатов диссертации.

Результаты работы были представлены и обсуждались на таких конференциях:

- ежегодные итоговые научные конференции Института проблем регистрации информации НАН Украины (2008 и 2014 гг.);

- 6-я Международной конференции “Современные компьютерные системы и сети: разработка и применение” (Киев, 2013);

- 10-я и 16-я международные научно-технические конференции “Системный анализ и информационные технологии” (Киев, 2008 и 2014 гг.).

Публикации. Результаты диссертационной работы опубликованы в 20 научных работах, включая 1 монографию; 9 статей в научно-технических изданиях, утвержденных МОН Украины: “Электронное моделирование”, “Реєстрація, зберігання і обробка даних”, “Радіоелектронні і комп’ютерні

системи”, “Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка” (в том числе, 4 статьи, которые реферируются наукометрическими базами данных eLIBRARY.RU, Index Copernicus, Cambridge Scientific Abstracts, Computer and Information Systems Abstracts, INIS Collection); 4 публикации в иностранном электронном издании ArXiv, которые входят в реферативную базу Citebase; 6 тезисов докладов научно-технических конференций.

Объем и структура диссертации. Диссертация состоит из введения, четырех разделов, выводов, списка использованной литературы и четырех приложений. Работа включает 143 страницы основного текста, 23 рисунка, 5 таблиц, 115 наименований литературных источников.

Во введении обоснована актуальность проблемы представления информации с помощью неканонических гиперкомплексных чисел и их практического применения. Сформулировано цель и задачи исследования, определены научная новизна и практическое значение полученных результатов.

Первый раздел «Анализ форм представления данных в математическом моделировании» носит посвящен анализу форм представления данных, в том числе, гиперкомплексной формы представления данных, ее использования и особенностей. Рассмотрены основные свойства, операции и классификационные признаки ГЧС, в том числе признак каноничности системы. В диссертационной работе уделено особое внимание неканоническим ГЧС как наиболее перспективным и наименее изученным.

Второй раздел «Развитие теоретических основ синтеза и анализа неканонических гиперкомплексных числовых систем» посвящен модификации существующих методов перечисления неканонических ГЧС, обработке и анализу полученных результатов. Рассмотрены вопросы множественности неканонических ГЧС: исследованы классы изоморфизма для неканонических ГЧС размерности 2, предложены методы перехода от бесконечномерной гиперкомплексной системы к конечномерным неканоническим ГЧС путем

факторизации. В разделе также исследованы методы выполнения основных операций в неканонических ГЧС и изоморфных им системах.

В третьем разделе, «Свойства неканонических гиперкомплексных числовых систем и операции в них», рассмотрены такие алгебраические характеристики неканонических ГЧС, как единичный элемент, норма, сопряженные, делители нуля, усовершенствованы методы их определения для неканонических ГЧС. Исследованы вычислительные сложности алгоритмов определения арифметических характеристик для разных числовых систем. Предложена метод вычисления наименьших вычетов в неканонических ГЧС. Промоделирован алгоритм Евклида с представлением исходных данных в неканонических ГЧС, определена его вычислительная сложность.

Четвертый раздел «Решение практических задач с применением неканонических гиперкомплексных числовых систем» посвящен математическому моделированию задачи разделения секрета и синтеза реверсивного цифрового фильтра с представлением данных в неканонических ГЧС.

Расширена задача разделения секрета для неканонических ГЧС третьей и четвертой размерности. Предложен способ восстановления информации с применением алгоритма Евклида. Исследованы и сопоставлены средние данные по количеству операций при моделировании представления исходных данных, разделения и восстановления секрета с использованием канонических и неканонических ГЧС. Показано, что применение неканонических ГЧС позволяет существенно снизить количество операций для модели разделения секрета в неканонических ГЧС, начиная с размерности 4 (в среднем на 44%), при сохранении такой же криптостойкости.

Разработана математическая модель реверсивного цифрового фильтра с гиперкомплексными коэффициентами. Предложен и реализован метод синтеза структур неканонических ГЧС, которые могут быть использованы для построения цифрового фильтра. Предложен метод оптимизации цифрового

фильтра по параметрической чувствительности. Сопоставлены суммарные параметрические чувствительности цифровых фильтров с вещественными и гиперкомплексными коэффициентами. Показано существенное снижение параметрической чувствительности эквивалентного фильтра с вещественными коэффициентами (до ~50%) и существующих фильтров с гиперкомплексными коэффициентами (до ~40%).

РАЗДЕЛ 1. АНАЛИЗ ФОРМ ПРЕДСТАВЛЕНИЯ ДАННЫХ В МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ

1.1. Формы представления информации в математическом моделировании и их применения

В настоящее время объемы данных, подлежащие обработке, неуклонно растут вместе с ростом мощностей вычислительных систем. Несмотря на то, что в настоящее время происходит довольно активное развитие аппаратной части вычислительных систем, вопрос быстродействия алгоритмов, оперирующих большими массивами данных, является актуальным, так как размерность решаемых задач на таких системах также растет.

Оценка сложности алгоритма базируется на нескольких факторах [38-39]. «Во многих случаях в качестве меры сложности вычислений берется количество арифметических операций в алгоритме. Хотя и существует грубое соответствие между общей и арифметической сложностью алгоритма, все же практическая ценность вычислительного метода зависит от многих факторов. Эффективность алгоритма определяется не только числом операций, но и такими параметрами, как число перемещений данных, стоимость вспомогательных операций, общая структурная сложность, различные возможности, представляемые используемой вычислительной системой, искусство программиста. Поэтому упорядочение алгоритмов по их действительной эффективности, выраженной временем выполнения, является весьма трудным делом, так что сравнения, основанные лишь на числе арифметических операций, должны быть «взвешены» с учетом факторов, возникающих при конкретных реализациях этих алгоритмов». [40]

Часто в основе ускорения алгоритма лежит специальная организация входных данных в виде той или иной формы их представления. Например, вместо того, чтобы повысить быстродействие процессора, можно организовать вычисления для некоторых задач таким образом, чтобы текущего

быстродействия процессора оказалось достаточно. Этим и обусловлен выбор формы представления массивов данных.

Традиционно, под формой представления данных, понимают способ отображения чисел и символов в памяти вычислительной машины, например, в двоичной системе счисления, реже – в шестнадцатеричной. Также различают представление чисел в формате с плавающей и фиксированной точкой. В данной же работе рассматриваются структурные формы представления массивов данных, которые, в свою очередь, для представления каждого элемента такого массива, могут использовать любую традиционную форму представления.

Рассмотрим некоторые структурные формы представления данных, которые сегодня широко используются в практических задачах:

1. Векторно-матричная форма представления данных, которая используется повсеместно. Данная форма является универсальным способом представления информации, однако, как правило, универсальность требует использования избыточных ресурсов для выполнения некоторых задач.

Например, матричную форму можно использовать для представления базисных элементов комплексного числа [40]:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow 1 ; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Leftrightarrow i.$$

Тогда комплексное число $A = a_1 + i * a_2$ можно представить в виде:

$$A = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} * \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}.$$

Но в этом случае, умножение таких чисел сводится к дополнительным операциям умножения и сложения.

2. Полиномиальная форма представления данных. Техническая простота вычислений, связанных с многочленами, по сравнению с более сложными классами функций, способствовали развитию методов разложения в ряды и полиномиальной интерполяции в математическом анализе.

Многочлены также играют ключевую роль в алгебраической геометрии, объектом которой являются множества, определённые как решения систем многочленов. Особые свойства преобразования коэффициентов при умножении многочленов используются в алгебраической геометрии, алгебре, теории узлов и других разделах математики для кодирования, или выражения многочленами свойств различных объектов [41].

В практических же задачах, полиномиальная форма представления информации широко используется в быстрых алгоритмах обработки сигналов, в частности, произведение многочленов используется для представления сверток; в обработке изображений, распознавании образов и прогнозировании, принятии решений, моделировании дискретных устройств и т.д. Практический интерес представляют полиномиальные формы, которые имеют однородную алгебраическую структуру и хорошо реализуются средствами современной микроэлектроники. Также, в быстрых алгоритмах обработки сигналов и изображений при выполнении вычислительных процедур широко используются интерполяционные полиномы Лагранжа, как форма представления информации, что позволяет минимизировать количество выполняемых элементарных операций [40-41].

Например, линейную свертку можно записать через многочлены. Для заданных двух последовательностей: $d = \{d_i, i = 0, \dots, N-1\}$ (последовательности данных) и $g = \{g_i, i = 0, \dots, L-1\}$ (последовательности фильтра), где N - длина блока данных, а L - длина фильтра. Линейной сверткой называется новая последовательность:

$$s = \{s_i, i = 0, \dots, L + N - 2\},$$

элементы которой определяются равенством

$$s_i = \sum_{k=0}^{N-1} g_{i-k} d_k, i = 0, \dots, L + N - 2.$$

Тогда можно записать свертку через многочлены:

$$s(x) = g(x)d(x),$$

$$\text{где } s(x) = \sum_{i=0}^{L+N-1} s_i x^i, \quad d(x) = \sum_{i=0}^{N-1} d_i x^i, \quad g(x) = \sum_{i=0}^{L-1} g_i x^i \quad [22-23].$$

В практических задачах встречается применение полиномиальной системы остаточных классов, как одного из способов распараллеливания вычислений или же минимизации количества элементарных операций [40].

3. Рассмотрим другую форму представления информации, такую как системы остаточных классов. Преимуществом системы остаточных классов является то, что в ней возможно распараллеливание вычислений, при этом оперируя с меньшими числами. Также китайская теорема об остатках гарантирует однозначность представления чисел на конкретном диапазоне [42]. Недостатками можно считать ограниченность представления чисел и громоздкость перевода из позиционной системы счисления в систему остаточных классов и обратно. Однако, при достаточном количестве операций алгоритма именно в системе остаточных классов, затратами на перевод из одной системы в другую можно пренебречь.

Системы остаточных классов широко используются в микроэлектронике в специализированных устройствах цифровой обработки сигналов и изображений, в частности, в алгоритмах быстрых преобразований Фурье, а также в вычислениях, где требуется контроль ошибок, за счет введения дополнительных избыточных модулей, и высокая скорость работы, которую обеспечивает параллельная реализация базовых арифметических операций [42, с. 71-75]. Китайская теорема об остатках до сих пор широко используется в криптографии, являясь основой многих алгоритмов шифрования с открытым ключом [43-45]. Подробнее применение систем остаточных классов в практических задачах будет рассмотрено в следующих главах.

Наряду с вышеупомянутыми структурными формами представления информации, особый интерес представляет гиперкомплексная форма представления данных, определение которой будет рассмотрено далее. Примеры применения известных и широко используемых в теории гиперкомплексных числовых систем комплексных, двойных, дуальных чисел,

кватернионов и др. для повышения эффективности алгоритмов в совершенно различных областях науки и техники известны достаточно давно. Рассмотрим некоторые из них:

1. Для моделирования вращения и перемещения используются дуальные числа, бикватернионы и двойные кватернионы, которые нашли широкое применение в задачах моделирования и управления плоскими механизмами [46-48], роботами и манипуляторами с многими степенями свободы [49-51] и даже моделировании скелета человека [52].

2. Кватернионы эффективно используются в задачах управления ориентацией твердого тела [53]. В отличие от других параметров ориентации компоненты-параметры классических нормированных кватернионов имеют такую совокупность свойств и особенностей, что обеспечивает им в настоящее время приоритетное использование в таких задачах, а именно:

- компоненты классических нормированных кватернионов – параметров Эйлера не вырождаются, т.е. не обращаются в бесконечность, при любом положении твердого тела;

- система из четырех кинематических дифференциальных уравнений вращения твердого тела, записанная в параметрах кватерниона вращения, имеет линейный вид;

- по параметрам кватерниона может быть всегда однозначно определен угол конечного поворота твердого тела от нуля до 2π [54-55].

Таким образом, вышеуказанные преимущества существенно упрощают задачу численного интегрирования кинематических дифференциальных уравнений и обеспечивают эффективное решение задач управления ориентацией твердого тела.

Вышеперечисленные преимущества позволяют использовать кватернионы для решения задач компьютерной графики и создания эффектов анимации [56], обработки цветного изображения [57]. В таких работах, как [58-

59] исследованы задачи деформации упругих и эластичных конструкций с использованием кватернионов.

3. Еще одной областью эффективного применения гиперкомплексной формы представления данных является криптография. Например, наряду с вышеуказанной полиномиальной формой остаточных классов, может использоваться гиперкомплексная форма в алгоритмах шифрования с открытым ключом. Таким образом, используя переходы из вещественной формы в гиперкомплексную, можно строить в последней систему остаточных классов, и строить алгоритмы, которые будут обладать более высокой стойкостью. Необходимо отметить, что гиперкомплексные числовые системы больших порядков, а особенно неканонические гиперкомплексные числовые системы, усложняют вычисления, как и сложный алгоритм изоморфного перехода из одной системы в другую. Поэтому ключевым моментом является выбор конкретной гиперкомплексной числовой системы, с представлением данных в которой, можно будет как существенно повысить устойчивость криптографического алгоритма, так и минимизировать дополнительные затраты, связанные на его реализацию в гиперкомплексной числовой системе [53-57].

4. Широко применяются гиперкомплексные числа и для повышения эффективности цифровой обработки сигналов. Традиционно, в быстрых алгоритмах обработки сигналов могут использоваться комплексные коэффициенты для минимизации элементарных операций. Например, в работах [65-74] рассмотрены фильтры с гиперкомплексными коэффициентами, которые при равных условиях, обеспечивают работу фильтра на значительно высшей тактовой частоте, по сравнению с фильтром с вещественными коэффициентами.

1.2. Гиперкомплексная форма представления информации; неканонические гиперкомплексные числовые системы

Подробные сведения о гиперкомплексных числовых системах можно найти в [19-26] и других работах. Приведем основные определения, на которых будут основываться дальнейшие исследования.

С алгебраической точки зрения гиперкомплексная числовая система – это кольцо с структурой векторного пространства, то есть, гиперкомплексной числовой системой размерности n называется множество чисел такого вида:

$$A = a_1 E_1 + a_2 E_2 + \dots + a_n E_n, \quad (1.1)$$

с определенными правилами выполнения операций сложения и умножения.

Совокупность элементов

$$\{E_1, E_2, \dots, E_n\} \quad (1.2)$$

называется базисом гиперкомплексной числовой системы или системы ее образующих.

Коэффициенты $A = a_1, a_2, \dots, a_n$ могут принадлежать системам вещественных, комплексных или других гиперкомплексных чисел, в том числе и рассматриваемой гиперкомплексной числовой системе. В этом случае считается, что гиперкомплексная числовая система задана над соответствующей системой вещественных, комплексных чисел или другой числовой системой.

Для определения правил выполнения операции умножения, и, соответственно, полного задания гиперкомплексной числовой системы необходимо задать правила умножения элементов базиса (1.2), такие чтобы числовая система должна быть замкнута относительно этой операции [1].

В общем виде произведение двух базисных элементов с (1.2) из-за замкнутости системы относительно операции умножения должно представлять собой число такой же гиперкомплексной числовой системы вида (1.1):

$$E_i E_j = \sum_{k=1}^n \gamma_{ij}^k E_k \quad (1.3)$$

Коэффициенты γ_{ij}^k , которые называют структурными константами, являются вещественными числами: $\gamma_{ij}^k \in \mathcal{R}$. При таком представлении для полного определения гиперкомплексной числовой системы необходимо задать n^3 структурных констант.

Простейшие операции в гиперкомплексной числовой системе это сложение и умножение. Сложение производится покомпонентно:

$$A + B = \sum_{i=1}^n (a_i + b_i) E_i. \quad (1.4)$$

В том случае, если в базисе присутствует единичный элемент системы, то без ограничения общности, им можно считать элемент E_1 .

Умножение гиперкомплексных чисел производится путем их перемножения как полиномов, подстановкой произведения базисных элементов по заданным правилам (1.3). В общем виде, произведение будет иметь вид:

$$A \cdot B = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n a_i b_j \gamma_{ij}^k E_k. \quad (1.5)$$

Деление двух гиперкомплексных чисел производится с помощью формулы:

$$C = \frac{A}{B} = \frac{\sum_{i=1}^n a_i E_i}{\sum_{j=1}^n b_j E_j} = \frac{A \cdot \bar{B}}{B \cdot \bar{B}} = \frac{A \cdot \bar{B}}{N(B)}, \quad (1.6)$$

где $N(B)$ - норма знаменателя, а \bar{B} - сопряженный знаменателю элемент. Понятие сопряженного элемента будет рассмотрено подробнее в третьем разделе.

Два гиперкомплексных числа равны, если попарно равны соответствующие коэффициенты при одинаковых базисных элементах, а именно:

$$A = B, \text{ если } a_i = b_i, \quad i = 1, \dots, n.$$

В гиперкомплексных числовых системах вводится понятия единичный и нулевой элементы.

Нулевой элемент ГЧС или ноль – это гиперкомплексное число, удовлетворяющее требованию [24]:

$$A + 0 = 0 + A = A.$$

Гиперкомплексное число равняется нулю, если коэффициенты при всех базисных элементах равны нулю:

$$A = 0, \text{ если } a_i = 0, \quad i = 1, \dots, n.$$

Единичный элемент ГЧС, или единица – это гиперкомплексное число ξ , для которого выполняется соотношение:

$$A \cdot \xi = A \cdot \xi = A.$$

Единичный элемент может быть элементом базиса числовой системы, как например, в комплексных числах, кватернионах, октавах и многих других гиперкомплексных числовых системах. Более подробно единичный элемент будет рассмотрен в 3-й главе.

В данное время не существует общепринятой классификации гиперкомплексных числовых систем. Поэтому рассмотрим некоторые наиболее важные классификационные признаки:

- размерность;
- свойства закона композиции;
- структурные особенности;
- принадлежность классу изоморфизма;
- каноничность;
- присутствие в базисе единичного элемента;

- наличие в системе делителей нуля и делителей единицы.

Размерность гиперкомплексной числовой системы определяется максимальным количеством линейно независимых элементов системы, которая равняется количеству элементов в базисе системы. Систему вещественных чисел можно рассматривать как числовую систему 1-ой размерности.

В зависимости от свойств закона композиции, то есть операции умножения, множество гиперкомплексных чисел распадается на ряд классов [1-3]. Например, это класс коммутативных, некоммутативных и антикоммутативных гиперкомплексных числовых систем, для которых выполняется, соответственно:

$$\begin{aligned} ab &= ba, & a, b \in \Gamma, \\ ab &\neq ba, & a, b \in \Gamma, \\ ab &= -ba, & a, b \in \Gamma. \end{aligned}$$

Рассмотрим свойство ассоциативности умножения. Гиперкомплексная числовая система ассоциативна, если для нее справедливо тождество:

$$(ab)c = a(bc), \quad a, b, c \in \Gamma. \quad (1.7)$$

В другом случае гиперкомплексная числовая система неассоциативна.

По структурным особенностям, гиперкомплексные числовые системы делятся на три типа:

- прямые суммы;
- сводимые путем линейных преобразований базиса к прямым суммам;
- не сводимые к прямым суммам.

Примером систем первого типа является система $R \oplus R$, таблица умножения которой имеет вид:

E_1	O
O	E_2

(1.8)

Фактически такая система является собой совокупность несвязанных между собой гиперкомплексных числовых систем. Структура таких систем значительно упрощает выполнение вычислительных процедур.

Система двойных чисел с базисными элементами e_1, e_2 представляет собой систему второго типа, с помощью линейных преобразований она превращается в систему (1.8):

$$\begin{aligned} E_1 &= \frac{1}{2}(e_1 + e_2) \\ E_2 &= \frac{1}{2}(e_1 - e_2) \end{aligned} \quad (1.9)$$

Если не существует невырожденного линейного преобразования с вещественными коэффициентами, которое превращает таблицу умножения системы в диагональную структуру, то это система третьего типа.

Линейное преобразование гиперкомплексной числовой системы приводит к базису другой числовой системы, которая отличается от исходной. Такие системы называют изоморфными или эквивалентными относительно линейного преобразования [1].

Понятие изоморфных гиперкомплексных числовых систем на основе невырожденного линейного преобразования базиса систем сформулировано в работе [20].

Необходимо отметить, что в соответствии с обобщенной теоремой Фробениуса: «Каждая обобщенная гиперкомплексная числовая система с делением изоморфна одной с четырех систем: системы вещественных чисел \mathbf{R} , комплексных чисел \mathbf{C} , системе кватернионов \mathbf{H} или системе октав \mathbf{Q} » [21].

Примером изоморфных систем можно назвать систему двойных чисел и диагональную, заданную таблицей (1.8). Преобразование, обратное (1.9), будет иметь вид [75]:

$$\begin{aligned} e_1 &= E_1 + E_2 \\ e_2 &= E_1 - E_2 \end{aligned}$$

Существование изоморфных систем наблюдается в числовых системах и более высоких размерностей.

Более подробно изоморфные преобразования будут рассмотрены в следующей главе. Необходимо отметить, что отношение изоморфизма объединяет некоторые гиперкомплексные числовые системы в классы, называемые классами изоморфизма [75].

Е.Штуди в своих работах ввел понятие «каноническая гиперкомплексная числовая система», то есть система, в которой произведение двух базисных элементов равняется какому-либо базисному элементу с коэффициентом ± 1 или 0 [20].

$$e_i \cdot e_j = \rho e_k, \quad i, j, k \in \{1, 2, \dots, n\}, \quad \rho = \pm 1, 0.$$

Структура и свойства канонических гиперкомплексных числовых систем достаточно хорошо изучены. Как показано выше, они нашли широкое применение в теоретических и практических аспектах. Данная же работа посвящена неканоническим гиперкомплексным числовым системам, рассмотрим этот класс и его особенности более подробно.

Введем определение неканонической гиперкомплексной числовой системы. Если хоть одно произведение базисных элементов является суммой двух или большего количества слагаемых и/или с коэффициентом, который не входит в множество $\{-1; 0; +1\}$, то такая гиперкомплексная числовая система называется неканонической.

Например, триплексные числа являются примером неканонической гиперкомплексной числовой системы 3-й размерности [76], у которой таблица умножения имеет вид:

E_1	E_2	E_3
E_2	$\frac{E_3 - E_2}{2}$	$-E_2$
E_3	$-E_2$	E_1

Триплексная числовая система является, по сути, единственной достаточно изученной неканонической гиперкомплексной числовой системой в наше время.

Неканонические гиперкомплексные числовые системы могут найти большое значение для решения как теоретических, так и практических задач. Так, например, неканонические гиперкомплексные числовые системы могут использоваться в решении таких теоретических задач, как перечисление классов изоморфизма. Практическое применение неканонических ГЧС также может быть разнообразным – от моделирования криптографических задач до синтеза цифровых фильтров. Более подробно основные аспекты неканонических гиперкомплексных числовых систем будут рассмотрены в следующих главах работы.

1.3. Методы построения алгебраических характеристик гиперкомплексных числовых систем

Для дальнейшей работы с гиперкомплексными числами необходимо рассмотреть основные алгебраические характеристики гиперкомплексных числовых систем, такие как норма и сопряжения, а также нелинейные функции гиперкомплексной переменной. В работах [77-81] эти вопросы рассмотрены более подробно.

1.3.1. Построение нормы и сопряжений гиперкомплексного числа.

Нормой гиперкомплексного числа является произведение самого числа и всех его сопряженных. Но с другой стороны, определение произведения сопряженных в общем виде требует определения нормы числа. Поэтому определение нормы опирается на следующие соображения, изложенные в [77-81].

Рассмотрим такое уравнение:

$$ax = b, \tag{1.10}$$

где $a, x, b \in \Gamma$, где Γ - какая-либо гиперкомплексная числовая система. То есть, с учетом (1.10)

$$\sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n (\gamma_{ij}^k a_i x_j) e_k = \sum_{k=1}^n b_k e_k, \quad (1.11)$$

Приравниваем выражения при одинаковых элементах базиса. Получим систему линейных уравнений:

$$\sum_{i=1}^n \sum_{j=1}^n \gamma_{ij}^k a_i x_j = b_k, k = 1, \dots, n.$$

Внутренние элементы $\sum_{i=1}^n \gamma_{ij}^k a_i$ можно представить элементами некоторой матрицы размерности $n \times n$. Обозначим ее через $N(a)$. Векторы-столбцы $(x_1, x_2, \dots, x_n)^T$ и $(b_1, b_2, \dots, b_n)^T$ обозначим соответственно \bar{x} и \bar{b} . Тогда (1.15) являет собой матричное уравнение:

$$N(a) \cdot \bar{x} = \bar{b}.$$

Детерминант матрицы $\|N(a)\|$ называется нормой числа a . Он зависит только от числа a и обладает всеми свойствами нормы.

Таким образом, норма гиперкомплексного числа a определяется за формулой:

$$N(a) = \left\| (N(a))_{j,k} = \sum_{i=1}^n \gamma_{ij}^k a_i \right\|_{j,k=1..n} \quad (1.12)$$

Обозначим сопряженные гиперкомплексного числа как $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{n-1}}$, а их произведение как \overline{a} . В общем случае для сопряженных $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{n-1}}$ должно выполняться уравнение:

$$a \cdot \overline{a_1} \cdot \overline{a_2} \cdot \dots \cdot \overline{a_{n-1}} = N(a) \cdot \xi, \quad (1.13)$$

где ξ – единичный элемент гиперкомплексной числовой системы. Или

$$a \cdot \overline{a} = N(a) \cdot \xi. \quad (1.14)$$

Допустим, что

$$\overline{a_k} = x_{1k} e_1 + x_{2k} e_2 + \dots + x_{nk} e_n \quad (1.15)$$

Если подставить (1.20) в (1.18) и приравнять выражения при одинаковых базисных элементах, получим систему из $(n-1)$ уравнений от $n(n-1)$ неизвестных [76-81]. Такая система не всегда имеет действительное решение. Поэтому, если неизвестен вид сопряженных и система уравнений не имеет решения в действительных числах, можно найти, с учетом (1.14), произведение сопряженных

$$\bar{a} = x_1 E_1 + x_2 E_2 + \dots + x_n E_n,$$

которое в основном и используется для вычислений.

1.3.2. Определение гиперкомплексной функции от гиперкомплексного аргумента.

Рассмотрим основные гиперкомплексные функции от гиперкомплексного аргумента, которые используются для решения прикладных задач.

Гиперкомплексной функцией $\Phi(X)$ от гиперкомплексного аргумента $X = \sum_{i=1}^n x_i e_i$ называется функция вида:

$$\Phi(X) = \sum_{i=1}^n \phi_i(x_1, x_2, \dots, x_n) \cdot e_i, \quad (1.16)$$

где $\phi_i(x_1, x_2, \dots, x_n)$, $i = 1, \dots, n$ - вещественная функция от вещественных аргументов [76].

Линейные функции от гиперкомплексной переменной имеют вид:

$$\Phi(X) = KX + C, \quad (1.17)$$

где $K \in \Gamma$.

Зная законы умножения и сложения в каждой системе, можно построить представление линейной функции от гиперкомплексной переменной. Соответственно, строим линейную функцию от гиперкомплексной переменной (1.22):

$$\Phi(X) = \sum_{i=1}^n \phi_i e_i = \sum_{i=1}^n \left(\sum_{j=1}^n \sum_{l=1}^n \gamma_{ij}^l k_l x_j + c_i \right) e_i.$$

Таким же образом представляются и некоторые простые нелинейные функции от гиперкомплексной переменной, такие как степенные, квадратичные и полиномы от гиперкомплексной переменной с гиперкомплексными коэффициентами [82-94].

Дробно-рациональная функция от гиперкомплексной переменной будет иметь вид:

$$\Phi(X) = \frac{\Phi_1(X)}{\Phi_2(X)} = \frac{K_1X + C_1}{K_2X + C_2} \quad (1.18)$$

При этом надо учитывать, что знаменатель $K_2X + C_2$ не может быть равным нулю и не может быть делителем нуля, а также потребуем, чтобы коэффициент K_1 тоже не был делителем нуля.

Функция (1.18) не выражена явно в гиперкомплексном виде (1.16), так как в знаменателе присутствует гиперкомплексное выражение. Для того чтобы привести выражение (1.18) к виду (1.16) следует умножить числитель и знаменатель на сопряженное число к знаменателю, то есть на выражение $\overline{K_2X + C_2}$. Тогда в знаменателе будет действительное число – норма, а в числителе произведение двух гиперкомплексных чисел, которое является числом гиперкомплексным.

Рассмотрим несколько различных функций от гиперкомплексной переменной [88-90].

Рассмотрим нелинейную функцию следующего вида:

$$\Phi(X) = \sqrt{X}, \quad (1.19)$$

где X - гиперкомплексное число.

Чтобы функция имела вид (1.21) необходимо возвести обе части уравнения (1.19) в квадрат, после чего имеем:

$$\Phi^2(X) = X, \quad (1.20)$$

а затем решить систему алгебраических уравнений относительно компонент гиперкомплексной переменной. По полученным компонентам можно построить гиперкомплексную функцию вида (1.16) с учетом ее многозначности [54].

Аналогично строятся функции, содержащие радикалы с любыми целыми показателями. Но в некоторых случаях искомое представление существует только при переходе от исходной ГЧС к ее удвоению системой комплексных чисел [54].

1.3.3. Построение представлений элементарных трансцендентных функций.

Представление элементарных трансцендентных функций от гиперкомплексной переменной строится на основании их представлений бесконечными рядами по аналогии с такими функциями с вещественными переменными:

а) экспонента

$$\text{Exp}(M) = E + \sum_{n=1}^{\infty} \frac{M^n}{n!}; \quad (1.21)$$

б) синус

$$\text{Sin}(M) = E + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{M^{2n-1}}{(2n-1)!}; \quad (1.22)$$

в) косинус

$$\text{Cos}(M) = E + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{M^{2n-2}}{(2n-2)!}; \quad (1.23)$$

д) гиперболический синус

$$\text{Sh}(M) = E + \sum_{n=1}^{\infty} \frac{M^{2n-1}}{(2n-1)!}; \quad (1.24)$$

е) гиперболический косинус

$$\text{Ch}(M) = \xi + \sum_{n=1}^{\infty} \frac{M^{2n-2}}{(2n-2)!}; \quad (1.25)$$

где $M \in \Gamma$, а ξ - единичный элемент гиперкомплексной системы Γ .

В некоторых случаях построение нелинейных функций как суммы бесконечных рядов производится непосредственно [54].

В общем случае приходится применять специальные методы:

- метод преобразования представления при помощи изоморфной гиперкомплексной системы [75];

- метод построения представления при помощи ассоциированной системы линейных дифференциальных уравнений [29-30].

Рассмотрим представление экспоненты при помощи линейных преобразований. Для примера возьмем систему двойных чисел, как прямую сумму вещественных систем $W_1 = R \oplus R$. В системе двойных чисел

$$X^n = (x_1 e_1 + x_2 e_2)^n = x_1^n e_1 + x_2^n e_2;$$

Так как единичный элемент в этой системе

$$\xi = e_1 + e_2,$$

То выражение (1.26) преобразуется в:

$$\text{Exp}(X) = \sum_{s=0}^{\infty} \frac{x^s}{s!} e_1 + \sum_{s=0}^{\infty} \frac{x^s}{s!} e_2 = e^{x_1} e_1 + e^{x_2} e_2.$$

Таким образом, данный подход можно применить для других систем, обладающих свойством изоморфизма.

Универсальным подходом является метод построения представления по ассоциированной системе линейных дифференцированных уравнений [54].

Рассмотрим, например, обычное линейное дифференциальное уравнение второго порядка.

$$\frac{d^2 Y}{dx^2} \pm M^2 Y = 0, \quad (1.26)$$

где $Y(x) = \sum_{i=0}^n y_i(x) e_i$ - гиперкомплексная функция скалярного аргумента,

$M, Y \in \Gamma$.

Если в (1.26) провести все действия с учетом закона композиции и приравнять все выражения с одинаковыми базисными компонентами, то получим систему линейных дифференциальных уравнений.

$$\frac{d^2 y_i}{dx^2} = a_{i1}y_1 + a_{i2}y_2 + \dots + a_{in}y_n, \quad i = 1, \dots, n. \quad (1.27)$$

Определим связь между (1.21)-(1.24) и системой (1.26). Поскольку эти ряды абсолютно сходятся, то их можно почленно дифференцировать. Продифференцируем дважды ряд для определения синуса (1.27), получим:

$$\frac{d^2 \text{Sin}(x)}{dx^2} = -M \text{Sin}(x). \quad (1.28)$$

Если подставить (1.28) в (1.27) со знаком “-”, то получим тождество. Это означает, что ряд для определения тригонометрического синуса удовлетворяет (1.27) со знаком “-”. Аналогично можно показать, что ряды (1.21)-(1.25) также будут решениями уравнения (1.26) с соответствующими знаками, и уравнение

$$\frac{d^2 Y}{dx^2} + M^2 Y = 0, \quad (1.29)$$

определяет тригонометрические функции, а уравнение

$$\frac{d^2 Y}{dx^2} - M^2 Y = 0 \quad (1.30)$$

гиперболические [54, 82-90].

Представление таких нелинейных функций, как экспонента, тригонометрические и гиперболические функции позволяет строить и обратные функции. Если обозначить прямую функцию через:

$$\Phi(X), \quad (1.31)$$

где $X = \sum_{j=1}^n x_j e_j$ - гиперкомплексная переменная, которая принадлежит гиперкомплексной числовой системе размерности n , а $\Phi^{-1}(Y)$ -обратная к (1.31) функция, то она будет определяться при помощи соотношения:

$$\Phi^{-1}(\Phi(X)) = X. \quad (1.32)$$

Соотношение (1.32) свидетельствует о том, что область значений прямой функции обязана входить в область существования обратной функции. Кроме того, область значений обратной функции должна входить в

гиперкомплексную числовую систему Γ . Этот факт необходимо иметь в виду, так как классические обратные функции, как правило, многозначны.

Представления экспоненты, гиперболических и тригонометрических функций [78], являются гиперкомплексными функциями, то есть имеют вид:

$$\Phi(X) = \sum_{j=1}^n \phi_j(x_1, \dots, x_n) \cdot e_j, \quad (1.33)$$

то есть:

$$\Phi^{-1}\left(\sum_{j=1}^n \phi_j(x_1, \dots, x_n) \cdot e_j\right) = \sum_{j=1}^n x_j \cdot e_j.$$

Для того, чтобы (1.33) было изображением обратной функции, ее аргумент должен быть просто гиперкомплексной переменной:

$$\sum_{j=1}^n \phi_j(x_1, \dots, x_n) \cdot e_j = \sum_{j=1}^n y_j \cdot e_j. \quad (1.34)$$

Если уравнение (1.34) представить в виде системы уравнений

$$\phi_j(x_1, \dots, x_n) = y_j, \quad j = 1, \dots, n, \quad (1.35)$$

то ее можно решить относительно переменных x_1, \dots, x_n .

Если эти решения подставить в (1.33), то получим изображение обратной функции [89-90]:

$$\Phi^{-1}\left(\sum_{j=1}^n y_j \cdot e_j\right) = \sum_{j=1}^n \varphi_j(y_1, \dots, y_n) \cdot e_j. \quad (1.36)$$

Функция вида (1.36) может быть многозначной. В этом случае необходимо выделить область главных значений, которая будет входить в гиперкомплексную числовую систему Γ .

Построение обратных тригонометрических и гиперболических функций основывается аналогичным образом на формулах (1.33)-(1.36) [92-95].

Построение нелинейных функций с гиперкомплексной переменной для некоторых неканонических гиперкомплексных числовых систем будут рассмотрены в следующих главах.

1.4. Анализ существующих моделей задач криптографии и обработки сигналов с представлением информации в гиперкомплексных числовых системах и постановка задачи дальнейших исследований

Как уже было отмечено, в ИПРИ НАН Украины уже исследовались математические модели задач криптографии и обработки сигналов с использованием гиперкомплексных числовых систем.

Рассмотрим модель пороговой схемы разделения секрета с представлением данных в канонических гиперкомплексных числовых системах [34, 60-62]. Исследования показали, что криптостойкость алгоритма возможно существенно улучшить используя представления информации в гиперкомплексном виде. При этом все вычисления и хранение ключей производятся в гиперкомплексных числах. Для улучшения криптостойкости алгоритма необходимо выбрать числовую систему со всеми ненулевыми ячейками в таблице умножения или же дальше наращивать размерность числовой системы, что, в свою очередь, увеличивает количество элементарных операций для выполнения разделения и восстановления секрета. Поэтому перспективным направлением исследований является представление исходных данных в неканонических гиперкомплексных числовых системах и, соответственно, модификация модели разделения секрета, что может позволить увеличить криптостойкость алгоритма без наращивания размерности такой системы, а, следовательно, минимизировать количество операций при выполнении работы такой модели с такой же криптостойкостью. Также, для моделирования задач криптографии важными вопросами являются исследование особенностей построения модулярной арифметики для неканонических гиперкомплексных числовых систем, а также моделирование и оптимизация алгоритмов, основанных на использовании модулярной арифметики, в частности алгоритма Евклида.

В работах [65-70] предложены модели эквивалентирования цифровых фильтров с вещественными коэффициентами цифровыми фильтрами с

гиперкомплексными коэффициентами. Эти модели рекурсивных фильтров с гиперкомплексными коэффициентами третьей и четвертой размерности в канонических ГЧС позволяют снизить суммарную параметрическую чувствительность фильтров на ~20% [35-37, 71-72]. Но поскольку множество систем, применимых к таким моделям, ограничено ввиду особых требований к ним, что более подробно рассмотрено в разделе 4, эквивалентирование цифрового фильтра с представлением коэффициентов в неканонических ГЧС дает широкие возможности для дальнейшей оптимизации фильтра по параметрической чувствительности. Для решения этой задачи также необходимо разработка метода построения неканонических ГЧС, удовлетворяющих критериям построения цифрового фильтра с коэффициентами в таких системах.

Важными теоретическими вопросами являются методы построения различных неканонических гиперкомплексных числовых систем, удовлетворяющих требованиям их использования в конкретных практических задачах.

Представление данных в неканонических ГЧС требует перехода из исходной области в гиперкомплексную, поэтому необходимо построение классов изоморфизма для таких систем, а также изучение их основных алгебраических характеристик и сложности алгоритмов их определения.

Использование неканонических ГЧС является важным направлением исследований, поскольку это может улучшить результаты моделирования задач, в которых используются канонические ГЧС.

Выводы по разделу 1.

Представление и обработка информации с использованием гиперкомплексных числовых систем играет все большую роль при математическом моделировании различных объектов и процессов. Гиперкомплексные числовые системы ставят перед исследователями значительные и интересные теоретические проблемы и порождают ряд практических применений в широком спектре приложений.

В разделе рассмотрены основные теоретические и практические аспекты представления данных в гиперкомплексных числовых системах, их текущее состояние и перспективы развития. Особое внимание уделено неканоническим ГЧС, с использованием которых возможно более эффективное решение ряда практических задач.

Проанализированы существующие модели задачи разделения секрета и синтеза цифрового фильтра с использованием гиперкомплексных числовых систем. Выделены основные преимущества таких подходов и недостатки с учетом того, что для этих моделей были использованы только канонические ГЧС. Рассмотрены направления дальнейших исследований для построения моделей вышеуказанных задач с использованием неканонических ГЧС.

РАЗДЕЛ 2. РАЗВИТИЕ ТЕОРЕТИЧЕСКИХ ОСНОВ СИНТЕЗА И АНАЛИЗА НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ

2.1. Разработка общего алгоритма перечисления неканонических гиперкомплексных числовых систем

Поскольку количество канонических и неканонических ГЧС какой-либо размерности очень велико, то для исследования их свойств можно говорить о задаче их перечисления и классификации.

Как известно, гиперкомплексная числовая система задается таблицей умножения. Классический перебор канонических гиперкомплексных числовых систем размерности n осуществляется путем последовательного перебора структурных элементов E_i , $i = 1..n$ в ячейках таблицы умножения.

E_{11}	E_{12}	\dots	E_{1n}
E_{12}	E_{22}	\dots	E_{2n}
\dots	\dots	\dots	\dots
E_{n1}	E_{2n}	\dots	E_{nn}

При этом коэффициенты при структурных элементах равны -1 , 0 или 1 , то есть $E_{ij} = -E_n, -E_{n-1}, \dots, 0, E_1, \dots, E_n$. Таким образом получаем $(2n+1)^{n^2}$ систем.

Примерами канонических гиперкомплексных числовых систем являются комплексные и квадриплексные числа.

Пример 2.1. Таблица умножения для системы комплексных чисел.

E_1	E_2
E_2	$-E_1$

Пример 2.2. Таблица умножения для системы квадриплексных чисел.

E_1	E_2	E_3	E_4
E_2	$-E_1$	E_4	$-E_3$
E_3	E_4	$-E_1$	$-E_2$
E_4	$-E_3$	$-E_2$	E_1

Перечисление неканонических гиперкомплексных числовых систем отличается от перечисления канонических систем. В каждой ячейке перебираются суммы структурных элементов, путем перебора коэффициентов при этих элементах [96-97].

$E_{111} + E_{112} +$ $+ \dots + E_{11n}$	$E_{121} + E_{122} +$ $+ \dots + E_{12n}$...	$E_{1n1} + E_{1n2} +$ $+ \dots + E_{1nn}$
$E_{211} + E_{212} +$ $+ \dots + E_{21n}$	$E_{221} + E_{222} +$ $+ \dots + E_{22n}$...	$E_{2n1} + E_{2n2} +$ $+ \dots + E_{2nn}$
...
$E_{n11} + E_{n12} +$ $+ \dots + E_{n1n}$	$E_{n21} + E_{n22} +$ $+ \dots + E_{n2n}$...	$E_{nn1} + E_{nn2} +$ $+ \dots + E_{nnn}$

где $E_{ijk} = C_{ij} \cdot E_k$, $C_{ij} \in \{-1, 0, 1\}$.

Таким образом получаем 3^{n^3} числовых систем, $(2n+1)^{n^2}$ из которых являются каноническими.

Пример 2.3 Таблица умножения неканонической ГЧС 2-й размерности

$E_1 + E_2$	E_2
E_2	$-E_1$

Пример 2.4 Таблица умножения неканонической ГЧС 3-й размерности

E_1	$-E_1$	$E_1 + E_4$
$-E_1 + E_3$	E_4	$-E_1$
E_4	$-E_3$	$E_2 - E_3$

Как уже было указано, перечисление можно осуществлять для тех гиперкомплексных числовых систем, которые заданы в общем виде. Вышеуказанные алгоритмы не учитывают коэффициенты в ячейках таблицы умножения отличные от единиц и нуля. Если коэффициенты выбраны из другого диапазона, количество полученных числовых систем возрастает соответственно количеству комбинаций таких коэффициентов. На рис. 2.1. показана блок-схема описанного алгоритма, а в Приложении В представлены листинги кода в системе MAPLE.

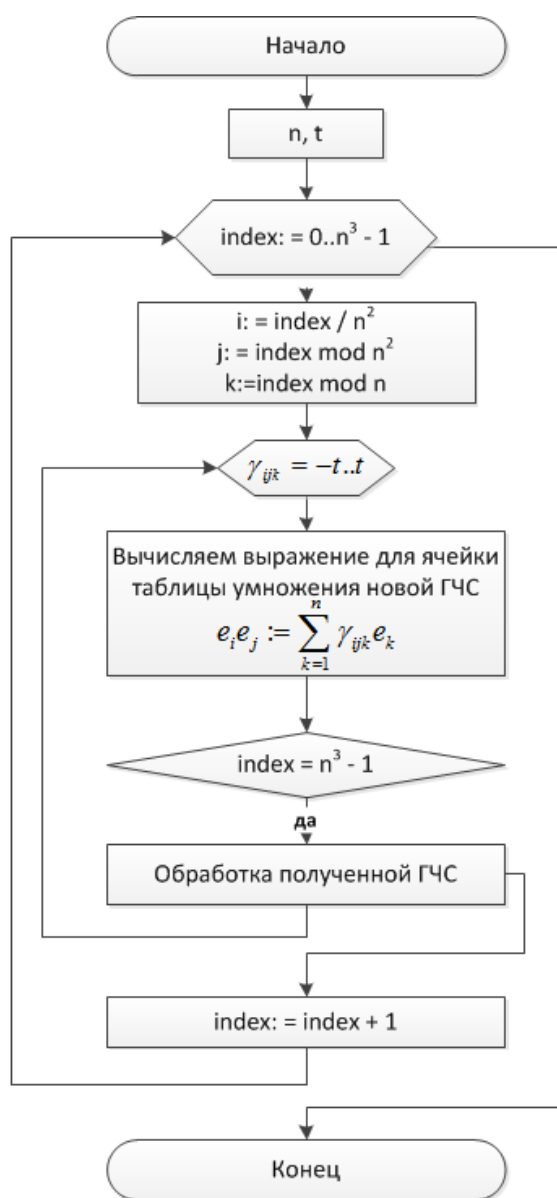


Рис. 2.1. Алгоритм построения неканонических ГЧС заданной размерности в общем виде.

2.2. Перечисление неканонических гиперкомплексных числовых систем изоморфных диагональным системам

Как уже было описано, известно множество задач, для решения которых используются сложные гиперкомплексные числовые системы. Их применение усложняет вычисления, поэтому для минимизации арифметических операций используют изоморфные переходы в более простые системы [54, 75, 95], например, диагональную вида $R \oplus \dots \oplus R$. Тем не менее, традиционно рассматриваемых канонических гиперкомплексных числовых систем, изоморфных диагональным, не так уж и много. Поэтому возникает необходимость поиска неканонических числовых систем, которые можно использовать для представления информации.

Понятие изоморфного перехода между двумя гиперкомплексными числовыми системами означает набор правил, с помощью которых число, представленное в одной числовой системе, можно перевести в другую числовую систему, а также сделать обратный переход с сохранением структуры самого числа.

Таким образом, получаем задачу по перечислению гиперкомплексных числовых систем – канонических и неканонических, изоморфных диагональной системе в виде прямой суммы вещественных чисел $R \oplus R \dots \oplus R$. При этом необходимо, чтобы для полученных систем выполнялось правило единицы [96-97]. Общий вид таблиц умножения рассматриваемых числовых систем будет иметь вид:

R_1	0	...	0
0	R_2	...	0
...
0	0	...	R_n

E_1	E_2	\dots	E_n
E_2	$a_{22}E_1 + b_{22}E_2 + \dots + k_{22}E_n$	\dots	$a_{n2}E_1 + b_{n2}E_2 + \dots + k_{n2}E_n$
\dots	\dots	\dots	\dots
E_n	$a_{2n}E_1 + b_{2n}E_2 + \dots + k_{2n}E_n$	\dots	$a_{nn}E_1 + b_{nn}E_2 + \dots + k_{nn}E_n$

Для этого используем перечисление гиперкомплексных числовых систем методом линейных преобразований. Суть алгоритма состоит в переборе коэффициентов при переменных в системе уравнений, с помощью которой осуществляется переход из искомой системы в диагональную, и затем получения правил умножения для полученной изоморфной системы.

Система уравнений для изоморфного перехода выглядит следующим образом [75, 97]:

$$\begin{cases} E_1 = A_1R_1 + B_1R_2 + \dots + K_1R_n = F_1(R_1, \dots, R_n) \\ E_2 = A_2R_1 + B_2R_2 + \dots + K_2R_n = F_2(R_1, \dots, R_n) \\ \dots \\ E_n = A_nR_1 + B_nR_2 + \dots + K_nR_n = F_n(R_1, \dots, R_n), \end{cases}$$

где A_i, B_i, K_i – вещественные коэффициенты.

Коэффициенты A_i, B_i, K_i при переменных перебираются в заранее заданном диапазоне с заданным шагом. Для увеличения количества полученных результатов можно расширять диапазон и уменьшать шаг. Для данного исследования использовался диапазон $-1 \dots 1$ и шаг 0.5 .

Необходимо отметить, что для найденных систем должно выполняться соответствие единичных элементов - $E_1 = R_1 + R_2 + \dots + R_n$, так как полученные системы должны быть с единицей в базисе. Это значит, то должны выполняться правила: $E_1 = E_1 \cdot E_1$, $E_2 = E_1 \cdot E_2$, ..., $E_n = E_1 \cdot E_n$. Закладываем это правило в формирование системы уравнений, т.е. фиксируем коэффициенты в первом уравнении системы: $A_1 = B_1 = \dots = K_1 = 1$.

Для того, чтобы определить, возможен ли изоморфный переход с помощью сгенерированной системы уравнений, проверяем, существует ли ее решение. Если решения в вещественных числах не существует, то найденная система не будет изоморфна заданной, т.е. не будет удовлетворять основному условию алгоритма.

Далее производим умножения уравнений полученной системы, и таким образом находим, чему равны умножения вида $E_i \cdot E_j$. Поскольку данный алгоритм учитывает только коммутативные системы, то $E_i E_j = E_j E_i$.

$$E_1 \cdot E_1 = f_{11}(R_1, \dots, R_n) = a_{11}F_1(R_1, \dots, R_n) + b_{11}F_1(R_1, \dots, R_n) + \dots + k_{11}F_n(R_1, \dots, R_n) = \\ = a_{11}E_1 + b_{11}E_2 + \dots + k_{11}E_n,$$

$$E_1 \cdot E_2 = f_{12}(R_1, \dots, R_n) = a_{22}F_2(R_1, \dots, R_n) + b_{22}F_2(R_1, \dots, R_n) + \dots + k_{22}F_2(R_1, \dots, R_n) = \\ = a_{22}E_1 + b_{22}E_2 + \dots + k_{22}E_n,$$

...

$$E_n \cdot E_n = f_{nn}(R_1, \dots, R_n) = a_{nn}F_n(R_1, \dots, R_n) + b_{nn}F_n(R_1, \dots, R_n) + \dots + k_{nn}F_n(R_1, \dots, R_n) = \\ = a_{nn}E_1 + b_{nn}E_2 + \dots + k_{nn}E_n.$$

Таким образом, получаем таблицу умножения для интересующей нас гиперкомплексной числовой системы. Производим дополнительные проверки. Прежде всего, отсеиваем системы, у которых не выполняется правило единичного элемента. То есть, проверяем равенство: $E_1 E_n = E_n$.

Также, для удобства модулярных вычислений, добавляем дополнительную проверку на целые коэффициенты при элементах в таблице умножения.

Пример 2.5.

Рассмотрим работу алгоритма на примере. Дана диагональная числовая система второй размерности:

R_1	0
0	R_2

Перебираем системы уравнений 2-й размерности:

$$E_1 = a_1 R_1 + b_1 R_2;$$

$$E_2 = a_2 R_1 + b_2 R_2.$$

Пусть $a_2 = 0.5$; $b_2 = -0.5$. Коэффициенты в первом уравнении равны единице $a_1 = b_1 = 1$.

Формируем одну из систем уравнений:

$$E_1 = R_1 + R_2;$$

$$E_2 = R_1 - R_2.$$

Затем находим произведения $E_{i,j}$.

$$E_1 E_1 = R_1 + R_2 = E_1;$$

$$E_1 E_2 = R_1 - R_2 = E_2;$$

$$E_2 E_2 = R_1 + R_2 = E_1.$$

Получаем систему с таблицей умножения:

E_1	E_2
E_2	E_1

Таблица удовлетворяет требованиям соблюдения правила единицы.

Пример 2.6.

Рассмотрим более сложный пример. Возьмем систему прямой суммы вещественных чисел размерности 3 и найдем неканоническую ГЧС изоморфную ей.

R_1	0	0
0	R_2	0
0	0	R_3

Перебираем коэффициенты для системы линейных уравнений.

Рассмотрим одну из полученных систем:

$$E_1 = R_1 + R_2 + R_3,$$

$$E_2 = -3R_1 - 2R_2 - R_3,$$

$$E_3 = R_1 + R_3.$$

Найдем умножения для $E_i E_j$ и подставляем в уравнения решения предыдущей системы:

$$E_1 \cdot E_1 = (R_1 + R_2 + R_3)(R_1 + R_2 + R_3) = R_1 + R_2 + R_3 = E_1;$$

$$E_1 \cdot E_2 = (R_1 + R_2 + R_3)(-3R_1 - 2R_2 - R_3) = -3R_1 - 2R_2 - R_3 = E_1;$$

$$\begin{aligned} E_2 \cdot E_2 &= (-3R_1 - 2R_2 - R_3)(-3R_1 - 2R_2 - R_3) = 9R_1 + 4R_2 + R_3 = \\ &= -4(R_1 + R_2 + R_3) - 4 \cdot (-3R_1 - 2R_2 - R_3) + (R_1 + R_3) = -4E_1 - 4E_2 + E_3; \end{aligned}$$

$$\begin{aligned} E_2 \cdot E_3 &= (-3R_1 - 2R_2 - R_3)(R_1 + R_3) = -3R_1 - R_3 = \\ &= 2(R_1 + R_2 + R_3) + (-3R_1 - 2R_2 - R_3) - 2(R_1 - R_3) = 2E_1 + E_2 - 2E_3; \end{aligned}$$

$$E_3 \cdot E_3 = (R_1 + R_3)(R_1 + R_3) = R_1 + R_3 = E_3.$$

Таким образом, получаем таблицу умножения для неканонической ГЧС размерности 3, изоморфной диагональной:

E_1	E_2	E_3
E_2	$-4E_1 - 4E_2 + E_3$	$2E_1 + E_2 - 2E_3$
E_3	$2E_1 + E_2 - 2E_3$	E_3

Пример 2.7.

Рассмотрим систему в виде прямой суммы вещественных чисел 4-й размерности.

R_1	0	0	0
0	R_2	0	0
0	0	R_3	0
0	0	0	R_4

Точно так же, как и в предыдущих примерах, перебираем системы линейных уравнений для изоморфных переходов. Рассмотрим одну из полученных систем:

$$E_1 = R_1 + R_2 + R_3 + R_4,$$

$$E_2 = -R_1 - R_2 - R_3 + R_4,$$

$$E_3 = R_2 + R_3 + R_4,$$

$$E_4 = R_1 + R_3 + R_4.$$

Найдем произведения для $E_i \cdot E_j$ и подставим в уравнения решения предыдущей системы:

$$E_1 \cdot E_1 = (R_1 + R_2 + R_3 + R_4)(R_1 + R_2 + R_3 + R_4) = R_1 + R_2 + R_3 + R_4 = E_1;$$

$$E_1 \cdot E_2 = (R_1 + R_2 + R_3 + R_4)(-R_1 - R_2 - R_3 + R_4) = -R_1 - R_2 - R_3 + R_4 = E_2;$$

$$E_1 \cdot E_3 = (R_1 + R_2 + R_3 + R_4)(R_2 + R_3 + R_4) = R_2 + R_3 + R_4 = E_3;$$

$$E_1 \cdot E_4 = (R_1 + R_2 + R_3 + R_4)(R_1 + R_3 + R_4) = R_1 + R_3 + R_4 = E_4;$$

$$E_2 \cdot E_2 = (-R_1 - R_2 - R_3 + R_4)(-R_1 - R_2 - R_3 + R_4) = R_1 + R_2 + R_3 + R_4 = E_1;$$

$$\begin{aligned} E_2 \cdot E_3 &= (-R_1 - R_2 - R_3 + R_4)(R_2 + R_3 + R_4) = -R_2 - R_3 + R_4 = \\ &= (R_1 + R_2 + R_3 + R_4) + (-R_1 - R_2 - R_3 + R_4) - (R_2 + R_3 + R_4) = E_1 + E_2 - E_3 \end{aligned}$$

$$\begin{aligned} E_2 \cdot E_4 &= (-R_1 - R_2 - R_3 + R_4)(R_1 + R_3 + R_4) = -R_1 - R_3 + R_4 = \\ &= (R_1 + R_2 + R_3 + R_4) + (-R_1 - R_2 - R_3 + R_4) - (R_1 + R_3 + R_4) = E_1 + E_2 - E_4 \end{aligned}$$

$$E_3 \cdot E_3 = (R_2 + R_3 + R_4)(R_2 + R_3 + R_4) = R_2 + R_3 + R_4 = E_3$$

$$\begin{aligned} E_3 \cdot E_4 &= (R_2 + R_3 + R_4)(R_1 + R_3 + R_4) = R_3 + R_4 = \\ &= -(R_1 + R_2 + R_3 + R_4) + (R_2 + R_3 + R_4) + (R_1 + R_3 + R_4) = -E_1 + E_2 + E_4 \end{aligned}$$

$$E_4 \cdot E_4 = (R_1 + R_3 + R_4)(R_1 + R_3 + R_4) = R_1 + R_3 + R_4 = E_4.$$

Таким образом, получаем таблицу умножения для неканонической гиперкомплексной числовой системы размерности 4, изоморфной диагональной:

E_1	E_2	E_3	E_4
E_2	E_1	$E_1 + E_2 - E_3$	$E_1 + E_2 - E_4$
E_3	$E_1 + E_2 - E_3$	E_3	$-E_1 + E_3 + E_4$
E_4	$E_1 + E_2 - E_4$	$-E_1 + E_3 + E_4$	E_4

Вышеописанный алгоритм был реализован и выполнен в пакете символьных вычислений MAPLE, блок-схема алгоритма представлена на рис.2.2. Листинг исходного кода процедур приведен в Приложении В.

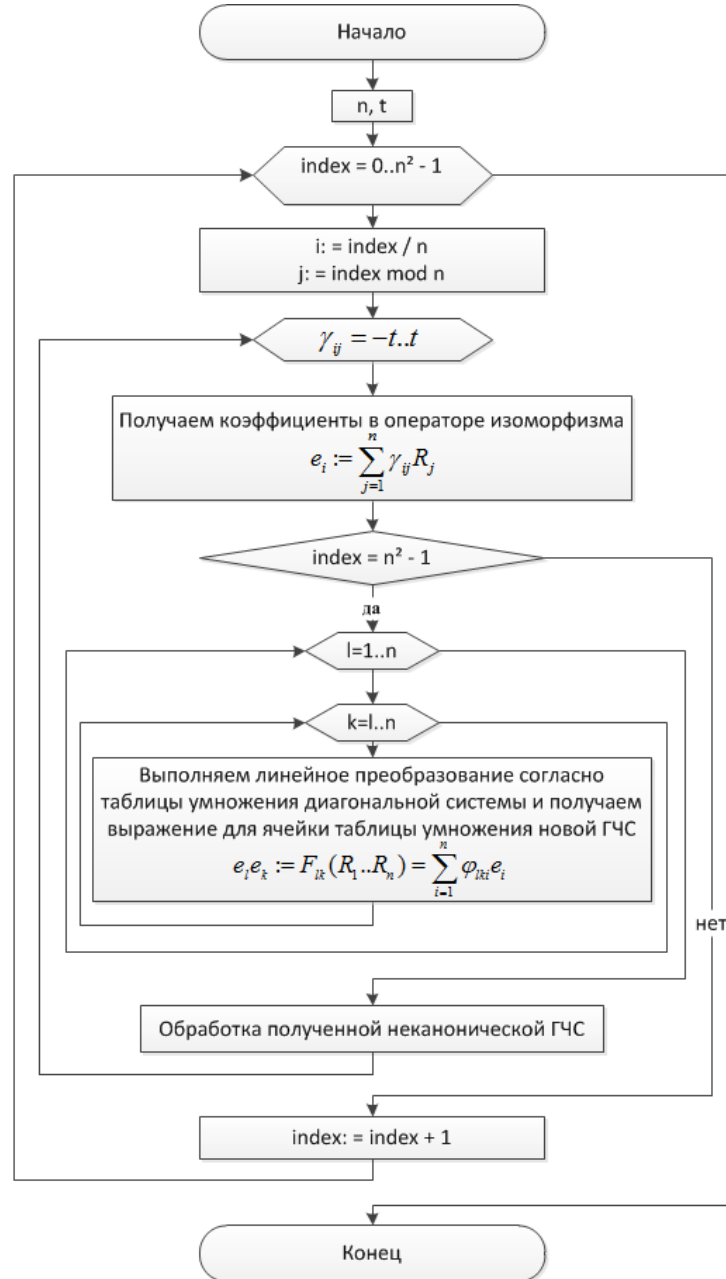


Рис. 2.2. Блок-схема алгоритма построения неканонических ГЧС изоморфных заданной.

2.3. Исследование некоторых классов изоморфизма неканонических гиперкомплексных числовых систем размерности 2

Рассмотрим свойство изоморфизма для неканонических гиперкомплексных числовых систем размерности 2 [98-99]. В самом общем виде, таблица умножения неканонической коммутативной ГЧС размерности 2 выглядит следующим образом:

$$\Gamma_2 = \begin{array}{|c|c|} \hline a_{11}E_1 + b_{11}E_2 & a_{12}E_1 + b_{12}E_2 \\ \hline a_{12}E_1 + b_{12}E_2 & a_{22}E_1 + b_{22}E_2 \\ \hline \end{array}, \quad (2.1)$$

где $a_{11}, a_{12}, a_{22}, b_{11}, b_{12}, b_{22}$ - вещественные числа.

Для того, чтобы таблица умножения (2.1) представляла собой гиперкомплексную систему, она должна иметь единичный элемент $X = x_1E_1 + x_2E_2$, а следовательно, существования нетривиального вещественного решения гиперкомплексного уравнения:

$$M = X \cdot M, \quad (2.2)$$

где $M = m_1E_1 + m_2E_2 \in \Gamma_2$.

Тогда, с учетом (2.2) получим систему уравнений:

$$\begin{cases} (m_1a_{11} + m_2a_{12})x_1 + (m_1a_{12} + m_2a_{22})x_2 = m_1 \\ (m_1b_{11} + m_2b_{12})x_1 + (m_1b_{12} + m_2b_{22})x_2 = m_1 \end{cases}$$

Откуда

$$\begin{aligned} x_1 &= \frac{b_{12}m_1^2 + (b_{22} - a_{12})m_1m_2 + a_{22}m_2^2}{(a_{11}b_{12} - b_{11}a_{12})m_1^2 + (a_{11}b_{22} - b_{11}a_{22})m_1m_2 + (a_{12}b_{22} - b_{12}a_{22})m_2^2}, \\ x_2 &= \frac{-b_{11}m_1^2 + (a_{11} - a_{12})m_1m_2 + a_{12}m_2^2}{(a_{11}b_{12} - b_{11}a_{12})m_1^2 + (a_{11}b_{22} - b_{11}a_{22})m_1m_2 + (a_{12}b_{22} - b_{12}a_{22})m_2^2}. \end{aligned} \quad (2.3)$$

Из (2.3) видно, что единичный элемент зависит от компонентов числа M , чего быть не должно. Избавиться от такой зависимости можно только когда коэффициенты квадратичных форм в числителях и знаменателях являются пропорциональными [99], то есть:

$$\frac{b_{12}}{a_{11}b_{12} - b_{11}a_{12}} = \frac{b_{22} - a_{12}}{a_{11}b_{22} - b_{11}a_{22}} = \frac{a_{22}}{a_{12}b_{22} - b_{12}a_{22}},$$

$$\frac{-b_{11}}{a_{11}b_{12} - b_{12}a_{12}} = \frac{a_{11} - b_{12}}{a_{11}b_{22} - b_{11}a_{22}} = \frac{a_{12}}{a_{12}b_{22} - b_{12}a_{22}}. \quad (2.4)$$

Будем считать константы a_{22}, b_{22} свободными, поскольку гиперкомплексные системы с такими структурными константами уже известны. Тогда получим систему из четырех уравнений с четырьмя неизвестными структурными константами, которая имеет такие решения:

$$1) \ a_{11} \in R, \ b_{11} = 0, \ a_{12} = 0, \ b_{12} = a_{11}, \ a_{22}, b_{22} \in R. \quad (2.5)$$

Это решение приводит к системе, которая представлена такой таблицей умножения:

$a_{11}E_1$	$a_{11}E_2$
$a_{11}E_2$	$a_{22}E_1 + b_{22}E_2$

(2.6)

Исходя из (2.2) получаем единичный элемент такой системы:

$$X = \frac{1}{a_{11}} E_1.$$

С помощью линейных преобразований базиса системы (2.6) мы можем перейти к изоморфной ей системе:

$$f_1 = \frac{1}{a_{11}} E_1; \ f_2 = E_2.$$

f_1	f_2
f_2	$a_{11}a_{22}f_1 + b_{22}f_2$

(2.7)

Тогда, в зависимости от знака величины $a_{11}a_{22} + \frac{b_{22}^2}{4}$, система (2.7) будет изоморфна системе комплексных, двойных или дуальных чисел.

$$2) \ b_{11} = 0, \ a_{12} = 0, \ a_{11} = b_{12} = b_{22}, \ a_{22} \in R \setminus \{0\}, \ b_{22} \in R.$$

Получим систему

$$\begin{array}{|c|c|} \hline b_{22}E_1 & b_{22}E_2 \\ \hline b_{22}E_2 & a_{22}E_1 + b_{22}E_2 \\ \hline \end{array}, \quad (2.8)$$

с единичным элементом

$$X = \frac{1}{b_{22}} E_1.$$

С помощью линейных преобразований базиса системы (2.8) можно перейти к изоморфной ей системе [86-88]:

$$f_1 = \frac{1}{b_{22}} E_1; f_2 = E_2.$$

$$\begin{array}{|c|c|} \hline f_1 & f_2 \\ \hline f_2 & a_{22}b_{22}f_1 + b_{22}f_2 \\ \hline \end{array}, \quad (2.9)$$

В зависимости от знака величины $a_{22}b_{22} + \frac{b_{22}^2}{4}$, система (2.9) изоморфна одной из систем комплексных, двойных или дуальных чисел.

Рассмотрим некоторые неканонические гиперкомплексные числовые системы размерности 2 диагонального вида:

$$\begin{array}{|c|c|} \hline \alpha_{11}f_1 + \beta_{11}f_2 & 0 \\ \hline 0 & \alpha_{22}f_1 + \beta_{22}f_2 \\ \hline \end{array}, \quad (2.10)$$

Рассмотрим правило единичного элемента для такой системы. Пусть единичный элемент имеет вид $X = x_1f_1 + x_2f_2$, тогда должно выполняться требование существования нетривиального вещественного решения уравнения (2.2), которое превращается в систему линейных уравнений:

$$\begin{cases} m_1\alpha_{11}x_1 + m_2\alpha_{22}x_2 = m_1 \\ m_1\beta_{11}x_1 + m_2\beta_{22}x_2 = m_1 \end{cases},$$

решение которой:

$$x_1 = \frac{\beta_{22}m_1m_2 + \alpha_{22}m_2^2}{(\alpha_{11}\beta_{22} - \beta_{11}\alpha_{22})m_1m_2},$$

$$x_2 = \frac{-\beta_{11}m_1^2 + \alpha_{11}m_1m_2}{(\alpha_{11}\beta_{22} - \beta_{11}\alpha_{22})m_1m_2}.$$

Как и в предыдущем случае, избавляемся от зависимости от компонентов числа M . Для этого необходимо выполнение условия: $\beta_{11} = \alpha_{22} = 0$. При этом, система (2.10) принимает вид:

$\alpha_{11}f_1$	0
0	$\beta_{22}f_2$

, (2.11)

а единичный элемент при этом имеет вид $X = \frac{1}{\alpha_{11}}f_1 + \frac{1}{\beta_{22}}f_2$.

Определим правила перехода из системы $R \oplus R$ в систему (2.9) [100-101]. Поскольку известны таблицы умножения обеих систем, необходимо определить коэффициенты в системе изоморфизма:

$$R_1 \cdot R_1 = R_1 = (y_{11}f_1 + y_{12}f_2)^2 = \alpha_{11}y_{11}^2f_1 + \beta_{22}y_{12}^2f_2 = y_{11}f_1 + y_{12}f_2$$

$$R_1 \cdot R_2 = 0 = (y_{11}f_1 + y_{12}f_2)(y_{21}f_1 + y_{22}f_2) = \alpha_{11}y_{11}y_{21}f_1 + \beta_{22}y_{12}y_{22}f_2 = 0,$$

$$R_2 \cdot R_2 = R_2 = (y_{21}f_1 + y_{22}f_2)^2 = \alpha_{11}y_{21}^2f_1 + \beta_{22}y_{22}^2f_2 = y_{21}f_1 + y_{22}f_2$$

что дает вещественную систему

$$\begin{cases} \alpha_{11}y_{11}^2 = y_{11} \\ \beta_{22}y_{12}^2 = y_{12} \\ \alpha_{11}y_{11}y_{21} = 0 \\ \beta_{22}y_{12}y_{22} = 0, \\ \alpha_{11}y_{21}^2 = y_{21} \\ \beta_{22}y_{22}^2 = y_{22} \end{cases}$$

у которой есть два решения:

$$1) \quad y_{11} = \frac{1}{\alpha_{11}}, y_{12} = 0, y_{21} = 0, y_{22} = \frac{1}{\beta_{22}};$$

$$2) \quad y_{11} = 0, y_{12} = \frac{1}{\beta_{22}}, y_{21} = \frac{1}{\alpha_{11}}, y_{22} = 0.$$

Оба решения дают невырожденное линейное преобразование, которое переводит систему $R \oplus R$ в систему (2.11). Для дальнейшего исследования будем использовать второе решение.

$$R_1 = \frac{1}{\beta_{22}} f_2, R_2 = \frac{1}{\alpha_{11}} f_1. \quad (2.12)$$

Теперь построим изоморфный переход от системы (2.1) к системе (2.11) с помощью промежуточного перехода в систему $R \oplus R$. Используем например систему (2.7) как частный случай системы (2.1). Тогда, оператор перехода из такого вида системы в систему прямой суммы вещественных чисел будет выглядеть таким образом [100-101] :

$$\begin{cases} E_1 = R_2, \\ E_2 = -\frac{b_{22}}{2k} R_1 + \frac{1}{k} R_2, \end{cases} \quad (2.13)$$

где $k^2 = a_{22}b_{22} + \frac{b_{22}^2}{4}$.

Учитывая (2.12)-(2.13) оператор перехода из (2.7) в (2.11) будет выглядеть так:

$$\begin{cases} E_1 = \frac{1}{\alpha_{22}} f_1, \\ E_2 = -\frac{b_{22}}{2k\beta_{22}} f_2 + \frac{1}{k\alpha_{22}} f_1. \end{cases}$$

2.4. Переход от бесконечномерной ГЧС к конечномерным ГЧС методами факторизации

Рассмотрим еще один подход получения множества неканонических гиперкомплексных систем - переход от бесконечномерной гиперкомплексной системы к конечномерным гиперкомплексным системам различных видов, в зависимости от правил умножения и метода факторизации [102].

Пусть Γ - дискретное счетное множество с бесконечным базисом $\{e_i\}, i=1, \dots, n, \dots$. На нем введена операция инволюции $*$ такая, что

$$*: \Gamma \rightarrow \Gamma, \text{ причем для } \forall e_i \in \Gamma \quad e_i^* \in \Gamma. \quad (2.15)$$

Существует элемент базиса $e_0 \in \Gamma$ такой, что

$$e_1 \cdot e_i = e_i \cdot e_1 = e_i, (e_i^*)^* = e_i \quad (2.16)$$

Операция умножения (свертка) в множестве производится согласно следующему правилу:

$$e_i \cdot e_j = \sum_{k=1}^{\infty} C_{ij}^k e_k. \quad (2.17)$$

Множество Γ является гиперкомплексной системой, которая может быть как дискретной, так и непрерывной, при выполнении условий (2.15)-(2.17).

Переход от бесконечномерной гиперкомплексной системы к конечномерным гиперкомплексным числовым системам будем осуществлять с учетом условий коммутативности и положительных структурных константах:

$$C_{ij}^k \geq 0; \quad C_{ii^*}^1 > 0; \quad C_{ij}^k = C_{ki^*}^j \geq 0. \quad (2.18)$$

Сформируем бесконечномерную гиперкомплексную систему, от которой впоследствии путем факторизации по конкретной подгруппе будем получать гиперкомплексные числовые системы различной размерности [102].

Задана группа $Z = \{-\infty, \infty\}$. На ней выбрана некоторая подгруппа автоморфизмов $V = \{-1, 1\} \in \text{Aut } Z$, что для $\forall n \in Z$, выполняются

$$1(n) = n \in Z, \quad -1(n) = -n \in Z.$$

Факторизуем группу Z по подгруппе V и получим множество $Z/V = \Gamma = N \cup \{0\}$. Определим для этого множества правило умножения базисных элементов (свертку).

Если для группы Z свертка имеет вид

$$\sigma_n \cdot \sigma_m = \sigma_{n+m}$$

или, учитывая свойства группы Z , можно записать $n \cdot m = n + m$.

Тогда свертка для $Z/V = \Gamma$ будет иметь вид:

$$\begin{aligned} n \cdot m &= \{n, -n\} \cdot \{m, -m\} = (n+m) + (m-n) + (-n-m) + (n-m) = \\ &= \{(n+m), -(n+m)\} + \{(n-m), -(n-m)\} \end{aligned}$$

Справедливо соотношение

$$\frac{1}{2}(\sigma_n \cdot \sigma_{-n}) = \sigma_n. \quad (2.19)$$

Получаем свертку:

$$\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_n + \sigma_{-n}) \cdot \frac{1}{2}(\sigma_m + \sigma_{-m}) = \frac{1}{4}(\sigma_{n+m} + \sigma_{-(n+m)}) + (\sigma_{|n-m|} + \sigma_{-|n-m|}) \quad (2.20)$$

Тогда вид свертки с учетом соотношения (2.19) имеет вид:

$$\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_{n+m} + \sigma_{|n-m|}) \quad (2.21)$$

Имея бесконечномерную гиперкомплексную систему и свертку, выбираем подгруппы, по которым будем осуществлять факторизацию.

Можно выбирать подгруппы $\{A_2, A_3, A_4, \dots\}$, где $A_2 = \{a_k : a_k = 2k, k \in \Gamma\}$, $A_3 = \{a_k : a_k = 3k, k \in \Gamma\}$, $A_4 = \{a_k : a_k = 4k, k \in \Gamma\}$ и т.д. При этом следует отметить, что каждая такая подгруппа является бесконечномерной и число таких подгрупп счетное количество.

После факторизации гиперкомплексной системы $\Gamma = N \cup \{0\}$ по подгруппе $A_2 = \{a_k : a_k = 2k, k \in \Gamma\}$ со сверткой (2.19) получим конечномерную гиперкомплексную числовую систему $G_2 = \Gamma/A_2 = \{e_1, e_2\}$ второй размерности, а именно, систему двойных чисел, таблица умножения которой имеет вид:

e_1	e_2
e_2	e_1

В дальнейшем, наращивая размерность, получаем неканонические ГЧС.

При факторизации гиперкомплексной системы $\Gamma = N \cup \{0\}$ по подгруппе $A_3 = \{a_k : a_k = 3k, k \in \Gamma\}$ со сверткой (2.21) получим ГЧС $G_3 = \Gamma/A_3 = \{e_1, e_2, e_3\}$ третьей размерности. Свертка полученной конечномерной гиперкомплексной числовой системы будет иметь вид:

e_1	e_2	e_3
e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_1 + e_2}{2}$
e_3	$\frac{e_1 + e_2}{2}$	$\frac{e_1 + e_2}{2}$

После факторизации гиперкомплексной системы $\Gamma = N \cup \{0\}$ по подгруппе $A_4 = \{a_k : a_k = 4k, k \in Q\}$ со сверткой вида (2.21) получим гиперкомплексную числовую систему $G_4 = \Gamma/A_4 = \{e_1, e_2, e_3, e_4\}$ четвертой размерности. Таблица умножения полученной гиперкомплексной числовой системы будет иметь вид:

e_1	e_2	e_3	e_4
e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_2 + e_4}{2}$	$\frac{e_1 + e_3}{2}$
e_3	$\frac{e_2 + e_4}{2}$	e_1	e_2
e_4	$\frac{e_1 + e_3}{2}$	e_2	$\frac{e_1 + e_3}{2}$

Так как в полученной гиперкомплексной числовой системе четвертой размерности есть закономерность, состоящая в следующем: $e_1 \cdot e_1 = e_1$, $e_3 \cdot e_3 = e_1$ то можно осуществить повторную факторизацию по подмножеству e_1, e_3 . Повторная факторизация $G_4/\{e_1, e_3\}$ приводит к гиперкомплексной числовой системе второй размерности с таблицей умножения

e_1	e_2
e_2	$\frac{e_1 + e_2}{2}$

После факторизации гиперкомплексной системы $\Gamma = N \cup \{0\}$ по подгруппе $A_5 = \{a_k : a_k = 5k, k \in \Gamma\}$ с правилами умножения вида (2.21) получим конечномерную ГЧС $G_5 = \Gamma/A_5 = \{e_1, e_2, e_3, e_4, e_5\}$ пятой размерности. При этом свертка полученной гиперкомплексной числовой системы будет иметь вид:

e_1	e_2	e_3	e_4	e_5
e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_2 + e_4}{2}$	$\frac{e_3 + e_5}{2}$	$\frac{e_1 + e_4}{2}$
e_3	$\frac{e_2 + e_4}{2}$	$\frac{e_1 + e_5}{2}$	$\frac{e_1 + e_2}{2}$	$\frac{e_2 + e_3}{2}$
e_4	$\frac{e_3 + e_5}{2}$	$\frac{e_1 + e_2}{2}$	$\frac{e_1 + e_2}{2}$	$\frac{e_2 + e_3}{2}$
e_5	$\frac{e_1 + e_4}{2}$	$\frac{e_2 + e_3}{2}$	$\frac{e_2 + e_3}{2}$	$\frac{e_1 + e_4}{2}$

Факторизуем гиперкомплексную систему $\Gamma = N \cup \{0\}$ по подгруппе $A_6 = \{a_k : a_k = 6k, k \in \Gamma\}$ аналогично предыдущим подгруппам и получим гиперкомплексную числовую систему $G_6 = \Gamma/A_6 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ шестой размерности. Свертка полученной гиперкомплексной числовой системы с учетом (2.21) будет иметь вид:

e_1	e_2	e_3	e_4	e_5	e_6
e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_2 + e_4}{2}$	$\frac{e_3 + e_5}{2}$	$\frac{e_4 + e_6}{2}$	$\frac{e_1 + e_5}{2}$
e_3	$\frac{e_2 + e_4}{2}$	$\frac{e_1 + e_5}{2}$	$\frac{e_2 + e_6}{2}$	$\frac{e_1 + e_3}{2}$	$\frac{e_2 + e_4}{2}$
e_4	$\frac{e_3 + e_5}{2}$	$\frac{e_2 + e_6}{2}$	e_1	e_2	e_3
e_5	$\frac{e_4 + e_6}{2}$	$\frac{e_1 + e_3}{2}$	e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_2 + e_4}{2}$
e_6	$\frac{e_1 + e_5}{2}$	$\frac{e_2 + e_4}{2}$	e_3	$\frac{e_2 + e_4}{2}$	$\frac{e_1 + e_5}{2}$

Так как в таблице умножения для этой ГЧС есть такие закономерности, что $e_1 \cdot e_1 = e_4 \cdot e_4 = e_1$, $e_1 \cdot e_2 = e_4 \cdot e_5 = e_2$, $e_1 \cdot e_3 = e_4 \cdot e_6 = e_3$, то можно выполнить повторную факторизацию полученной системы по подгруппе $\{e_1, e_4\}$. В результате получаем еще одну ГЧС третьей размерности со сверткой:

e_1	e_2	e_3
e_2	$\frac{e_1 + e_3}{2}$	$\frac{e_1 + e_2}{2}$
e_3	$\frac{e_1 + e_2}{2}$	$\frac{e_1 + e_3}{2}$

Аналогично получаем ГЧС более высоких размерностей. Как видно из приведенных выше примеров, получение ГЧС по подгруппам вида $A_4 = \{a_k : a_k = 4k, k \in \mathcal{Q}\}$, $A_6 = \{a_k : a_k = 6k, k \in \mathcal{Q}\}$ и т.д., то есть по подгруппам, элементы которых являются кратными 2, можно повторно факторизовать и получить ГЧС размерности в 2 раза меньше.

2.5. Метод синтеза конечномерных ГЧС путем факторизации бесконечномерной ГЧС с двухточечным представлением элементов

Рассмотрим теорию формирования двухточечной бесконечномерной гиперкомплексной системы, от которой потом путем факторизации по заданной подгруппе будем получать гиперкомплексные числовые системы различной размерности [54, 103].

Задана группа

$$Z^2 = \{(m, n) \in (-\infty; \infty), m > n\},$$

на которой рассмотрена некоторая подгруппа автоморфизмов

$$V_1 = \{e, \gamma\} \in \text{Aut}Z,$$

что для $\forall m, n \in Z^2$, выполняются условия:

$$e(m, n) = (m, n), \gamma(m, n) = (n, m) \in Z^2.$$

Факторизуем группу Z^2 по подгруппе V_1 и получим множество

$$Z^2/V_1 = \Gamma_1 = \{(m, n), (n, m)\}, m > n\}.$$

Далее определим для этого множества таблицу умножения базисных элементов. Если для группы Z^2 свертка имеет вид

$$\sigma_{(m,n)} \cdot \sigma_{(k,l)} = \sigma_{(m+k,n+l)}$$

или, учитывая свойства группы Z^2 , можно записать

$$(m, n) \cdot (k, l) = (m + k) + (n + l).$$

Тогда свертка для $Z^2/V_1 = \Gamma_1$ будет иметь вид:

$$(m, n) \cdot (k, l) = \{(m + k), (n + l)\} + \{(m + l), (n + k)\}$$

Справедливо соотношение

$$\frac{1}{2}(\sigma_{(m,n)} + \sigma_{(n,m)}) = \sigma_{(m,n)}. \quad (2.22)$$

Получаем свертку:

$$\begin{aligned} \sigma_{(m,n)} \cdot \sigma_{(k,l)} &= \frac{1}{2}(\sigma_{(m,n)} + \sigma_{(n,m)}) \cdot \frac{1}{2}(\sigma_{(k,l)} + \sigma_{(l,k)}) = \\ &= \frac{1}{4}[(\sigma_{(m+k,n+l)} + \sigma_{(n+k,m+l)} + \sigma_{(m+l,k+n)} + \sigma_{(n+l,m+k)})] = \frac{1}{2}(\sigma_{(m+k,n+l)} + \sigma_{(m+l,n+k)}) \end{aligned} \quad (2.23)$$

Поскольку выполняются условия (2.15-2.18), множество Γ_1 является гиперкомплексной системой. То есть множество $Z^2/V_1 = \Gamma_1$ является счетным, есть операция $*$ и она тривиальна: $n^* = n$, структурные константы $C_{ii^*}^0 = \frac{1}{2} > 0$ [54].

Имея бесконечномерную гиперкомплексную систему Γ_1 и свертку (2.23), выбираем подгруппы, по которым будем осуществлять факторизацию.

Выбираем подгруппы $A_2 = \{(2m, 2n), m, n \in \Gamma_1\}$, $A_3 = \{(3m, 3n), m, n \in \Gamma_1\}$, $A_4 = \{(4m, 4n), m, n \in \Gamma_1\}$ и т.д. Следует отметить, что каждая такая подгруппа является бесконечномерной и число таких подгрупп счетное количество.

Рассмотрим подгруппу $A_2 = \{(2m, 2n), m, n \in \Gamma_1\}$. Эта подгруппа является нормальной, так как выполняется свойство $p\Gamma_1 = \Gamma_1 p$ для всех $p \in \Gamma$.

То есть получаем

$$\begin{aligned}
(p_1, p_2)(2m, 2n) &= \frac{1}{2}((p_1, p_2) + (p_2, p_1)) \cdot \frac{1}{2}((2m, 2n) + (2n, 2m)) = \\
&= \frac{1}{4}((p_1 + 2m, p_2 + 2n) + (p_1 + 2n, p_2 + 2m) + (p_2 + 2m, p_1 + 2n) + (p_2 + 2n, p_1 + 2m)) = \\
&= \frac{1}{2}((p_1 + 2m, p_2 + 2n) + (p_2 + 2m, p_1 + 2n)).
\end{aligned}$$

С другой стороны,

$$\begin{aligned}
(2m, 2n)(p_1, p_2) &= \frac{1}{2}((2m, 2n) + (2n, 2m)) \cdot \frac{1}{2}((p_1, p_2) + (p_2, p_1)) = \\
&= \frac{1}{4}((p_1 + 2m, p_2 + 2n) + (p_1 + 2n, p_2 + 2m) + (p_2 + 2m, p_1 + 2n) + (p_2 + 2n, p_1 + 2m)) = \\
&= \frac{1}{2}((p_1 + 2m, p_2 + 2n) + (p_2 + 2m, p_1 + 2n)).
\end{aligned}$$

Факторизуем гиперкомплексную систему Γ_1 по подгруппе $A_2 = \{(2m, 2n), m, n \in \Gamma_1\}$ со сверткой (2.23). Как результат получим конечномерную гиперкомплексную числовую систему $\Gamma_1/A_2 = \{e_1, e_2, e_3, e_4\}$.

Причем $e_1 = (2m, 2n)$, $e_2 = (2m+1, 2n)$, $e_3 = (2m+1, 2n+1)$, $e_4 = (2m, 2n+1)$. Поскольку класс, соответствующий базисному элементу $e_4 = (2m, 2n+1)$ совпадает с классом, которому соответствует базисный элемент $e_2 = (2m+1, 2n)$, достаточно будет оставить один класс, например, $e_2 = (2m+1, 2n)$. В результате получим ГЧС третьей размерности, то есть $\Gamma_1/A_2 = G_1 = \{e_1, e_2, e_3\}$. Полученная система является неканонической, потому что свертка такой системы, с учетом (2.23), будет иметь вид:

e_1	e_2	e_3
e_2	$\frac{e_1 + e_3}{2}$	e_2
e_3	e_2	e_1

Рассмотрим подгруппу $A_3 = \{(3m, 3n), m, n \in \Gamma_1\}$. Эта подгруппа также является нормальной, так как выполняется свойство $p\Gamma_1 = \Gamma_1 p$ для всех $p \in \Gamma$.

После факторизации гиперкомплексной системы Γ_1 по подгруппе $A_3 = \{(3m, 3n), m, n \in \Gamma_1\}$ со сверткой (2.23) получим конечномерную гиперкомплексную числовую систему $\Gamma_1/A_3 = K_2 = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9\}$, при этом $e_1 = (3m, 3n)$, $e_2 = (3m, 3n + 1)$, $e_3 = (3m, 3n + 2)$, $e_4 = (3m + 1, 3n + 1)$, $e_5 = (3m + 2, 3n + 1)$, $e_6 = (3m + 2, 3n + 2)$, $e_7 = (3m + 1, 3n)$, $e_8 = (3m + 1, 3n + 2)$, $e_9 = (3m + 2, 3n)$. Класс, который соответствует базисному элементу $e_7 = (3m + 1, 3n)$, совпадает с классом, которому соответствует базисный элемент $e_2 = (3m, 3n + 1)$, поэтому достаточно оставить один базисный элемент $e_2 = (3m, 3n + 1)$. Таким же образом класс, соответствующий базисному элементу $e_3 = (3m, 3n + 2)$, совпадает с классом, которому соответствует базисный элемент $e_9 = (3m + 2, 3n)$, поэтому достаточно оставить один базисный элемент $e_3 = (3m, 3n + 2)$. А также класс, соответствующий базисному элементу $e_5 = (3m + 2, 3n + 1)$ совпадает с классом, которому соответствует базисный элемент $e_8 = (3m + 1, 3n + 2)$, поэтому достаточно оставить один базисный элемент $e_5 = (3m + 2, 3n + 1)$. Как результат, получаем гиперкомплексную числовую систему шестой размерности со сверткой (с учетом (2.23)):

e_1	e_2	e_3	e_4	e_5	e_6
e_2	$\frac{e_3 + e_4}{2}$	$\frac{e_1 + e_5}{2}$	e_5	$\frac{e_4 + e_6}{2}$	e_3
e_3	$\frac{e_1 + e_5}{2}$	$\frac{e_2 + e_6}{2}$	e_2	$\frac{e_3 + e_4}{2}$	e_5
e_4	e_5	e_2	e_6	e_3	e_1
e_5	$\frac{e_4 + e_6}{2}$	$\frac{e_3 + e_4}{2}$	e_3	$\frac{e_1 + e_5}{2}$	e_2
e_6	e_3	e_5	e_1	e_2	e_4

Полученную систему можно повторно факторизовать по подгруппе $\{e_1, e_4, e_6\}$. После повторной факторизации получим гиперкомплексную числовую систему третьей размерности с таблицей умножения:

e_1	e_2	e_3
e_2	e_3	e_1
e_3	e_1	e_2

Рассмотрим подгруппу $A_4 = \{(4m, 4n), m, n \in \mathcal{Q}_1\}$, которая также является нормальной, так как выполняется свойство $p\Gamma_1 = \Gamma_1 p$ для всех $p \in \Gamma$.

Факторизуем гиперкомплексную систему Γ_1 по подгруппе $A_4 = \{(4m, 4n), m, n \in \mathcal{Q}_1\}$ со сверткой (2.23) получим конечномерную ГЧС $\mathcal{Q}_1/A_4 = K_2 = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{13}, e_{14}, e_{15}, e_{16}\}$. Причем

$$e_1 = (4m, 4n), \quad e_2 = (4m, 4n + 1), \quad e_3 = (4m, 4n + 2), \quad e_4 = (4m, 4n + 3), \quad e_5 = (4m + 1, 4n + 1),$$

$$e_6 = (4m + 1, 4n + 2), \quad e_7 = (4m + 1, 4n + 3), \quad e_8 = (4m + 2, 4n + 2), \quad e_9 = (4m + 2, 4n + 3),$$

$$e_{10} = (4m + 3, 4n + 3), \quad e_{11} = (4m + 1, 4n), \quad e_{12} = (4m + 2, 4n), \quad e_{13} = (4m + 3, 4n),$$

$$e_{14} = (4m + 2, 4n + 1), \quad e_{15} = (4m + 3, 4n + 1), \quad e_{16} = (4m + 3, 4n + 2). \quad \text{Рассмотрим}$$

совпадающие классы при базисных элементах: $e_{11} = (4m + 1, 4n)$ и $e_2 = (4m, 4n + 1)$, $e_{12} = (4m + 2, 4n)$ и $e_3 = (4m, 4n + 2)$, $e_4 = (4m, 4n + 3)$ и $e_{13} = (4m + 3, 4n)$, $e_6 = (4m + 1, 4n + 2)$ и $e_{14} = (4m + 2, 4n + 1)$, $e_7 = (4m + 1, 4n + 3)$ и $e_{15} = (4m + 3, 4n + 1)$, $e_9 = (4m + 2, 4n + 3)$ и $e_{16} = (4m + 3, 4n + 2)$. Достаточно оставить представителей первых десяти несовпадающих классов.

Таким образом, получаем гиперкомплексную числовую систему десятой размерности. При этом закон умножения полученной гиперкомплексной числовой системы с учетом (2.23) будет иметь вид:

e_1	e_2	e_3	e_4	e_5	e_5	e_7	e_8	e_9	e_{10}
e_2	$\frac{e_3 + e_5}{2}$	$\frac{e_4 + e_6}{2}$	$\frac{e_1 + e_7}{2}$	e_6	$\frac{e_7 + e_8}{2}$	$\frac{e_2 + e_9}{2}$	e_9	$\frac{e_3 + e_{10}}{2}$	e_4
e_3	$\frac{e_4 + e_6}{2}$	$\frac{e_1 + e_7}{2}$	$\frac{e_2 + e_9}{2}$	e_7	$\frac{e_5 + e_9}{2}$	$\frac{e_5 + e_{10}}{2}$	e_3	$\frac{e_4 + e_6}{2}$	e_7
e_4	$\frac{e_1 + e_7}{2}$	$\frac{e_2 + e_9}{2}$	$\frac{e_3 + e_{10}}{2}$	e_2	$\frac{e_3 + e_5}{2}$	$\frac{e_4 + e_6}{2}$	e_6	$\frac{e_7 + e_8}{2}$	e_9

e_5	e_6	e_7	e_2	e_8	e_9	e_3	e_{10}	e_4	e_1
e_6	$\frac{e_7 + e_8}{2}$	$\frac{e_5 + e_9}{2}$	$\frac{e_3 + e_5}{2}$	e_9	$\frac{e_3 + e_{10}}{2}$	$\frac{e_4 + e_6}{2}$	e_4	$\frac{e_1 + e_7}{2}$	e_2
e_7	$\frac{e_2 + e_9}{2}$	$\frac{e_5 + e_{10}}{2}$	$\frac{e_4 + e_6}{2}$	e_3	$\frac{e_4 + e_6}{2}$	$\frac{e_1 + e_8}{2}$	e_7	$\frac{e_2 + e_9}{2}$	e_3
e_8	e_9	e_3	e_6	e_{10}	e_4	e_7	e_1	e_2	e_5
e_9	$\frac{e_3 + e_{10}}{2}$	$\frac{e_4 + e_6}{2}$	$\frac{e_7 + e_8}{2}$	e_4	$\frac{e_1 + e_7}{2}$	$\frac{e_2 + e_9}{2}$	e_2	$\frac{e_3 + e_5}{2}$	e_6
e_{10}	e_4	e_7	e_9	e_1	e_2	e_3	e_5	e_6	e_8

Можно повторно факторизовать данную гиперкомплексную систему по подгруппе элементов $\{e_1, e_5, e_8, e_{10}\}$. В результате повторной факторизации получим гиперкомплексную числовую систему четвертой размерности. Правила умножения такой системы будут иметь вид:

e_1	e_2	e_3	e_4
e_2	e_3	e_4	e_1
e_3	e_4	e_1	e_2
e_4	e_1	e_2	e_3

Можно определить закономерность получения размерности конечномерной ГЧС, исходя из вида выбранной подгруппы. Так для подгруппы $A_2 = \{(2m, 2n), m, n \in Q_1\}$ размерность получаемой ГЧС $|Q_1/A_2| = 3 = 4 - 1$, для подгруппы $A_3 = \{(3m, 3n), m, n \in Q_1\}$ размерность получаемой ГЧС $|Q_1/A_3| = 6 = 9 - 3$, для подгруппы $A_4 = \{(4m, 4n), m, n \in Q_1\}$ размерность получаемой ГЧС $|Q_1/A_4| = 10 = 16 - 6$ и т.д. Можно определить закономерность следующим образом:

$$|Q_1/A_k| = k^2 - |Q_1/A_{k-1}|.$$

2.6. Основные операции в неканонических ГЧС

Пусть задано два неканонических гиперкомплексных числа размерности n :

$$A = \sum_{i=1}^n a_i E_i \quad \text{и} \quad B = \sum_{i=1}^n b_i E_i. \quad (2.24)$$

Сумма и разность двух заданных неканонических гиперкомплексных чисел вычисляется таким же образом, как и для канонических гиперкомплексных чисел [24].

Произведение двух неканонических гиперкомплексных чисел равно:

$$C = A \cdot B = \left(\sum_{i=1}^n a_i e_i \cdot \sum_{j=1}^n b_j e_j \right) = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \gamma_{ij}^k a_i b_j e_k, \quad (2.25)$$

где γ_{ij}^k - структурная константа таблицы умножения заданной ГЧС.

Пример 2.8.

Пусть задана неканоническая ГЧС 2-й размерности:

E_1	E_2
E_2	$E_1 + E_2$

(2.26)

Пусть заданы два числа: $A = E_1 + 3E_2$ и $B = 2E_1 - 5E_2$. Произведение будет выглядеть таким образом:

$$C = A \cdot B = 1 \cdot 2 \cdot E_1 - 1 \cdot 5 \cdot E_2 + 2 \cdot 3 \cdot E_2 - 3 \cdot 5 \cdot E_1 - 3 \cdot 5 \cdot E_2 = -6E_1 - 7E_2$$

Пример 2.9.

Пусть задана система 4-й размерности:

E_1	E_2	E_3	E_4
E_2	$-E_2$	$-E_1 - E_2 - E_3$	$-E_1 - E_2 - E_4$
E_3	$-E_1 - E_2 - E_4$	$-E_3$	$-E_4$
E_4	$-E_1 - E_2 - E_3$	$-E_4$	$-E_4$

(2.27)

Покажем результат умножения в общем виде для чисел

$$A = a_1E_1 + a_2E_2 - a_3E_3 + a_4E_4 \text{ и } B = b_1E_1 + b_2E_2 - b_3E_3 + b_4E_4 :$$

$$\begin{aligned} C = A \cdot B &= a_1b_1E_1 + a_1b_2E_2 + a_1b_3E_3 + a_1b_4E_4 + a_2b_1E_2 - a_2b_2E_2 - a_2b_3(E_1 + E_2 + E_3) - \\ &- a_2b_4(E_1 + E_2 + E_4) + a_3b_1E_3 - a_3b_2(E_1 + E_2 + E_3) - a_3b_3E_3 - a_3b_4E_4 + a_4b_1E_4 - \\ &- a_4b_2(E_1 + E_2 + E_4) - a_4b_3E_4 - a_4b_4E_4 = \\ &= (a_1b_1 - a_2b_3 - a_2b_4 - a_3b_2 - a_4b_1)E_1 + (a_1b_2 + a_2b_1 - a_2b_2 - a_2b_3 - a_2b_4 - a_3b_2 - a_4b_1)E_2 + \\ &+ (a_1b_3 - a_2b_3 + a_3b_1 - a_3b_2 - a_3b_3)E_3 + (a_1b_4 - a_2b_4 - a_3b_4 + a_4b_1 - a_4b_2 - a_4b_3 - a_4b_4)E_4 \end{aligned}$$

Пусть задано два гиперкомплексных числа (1.1) порядка n . Частное от деления двух гиперкомплексных чисел равно:

$$C = \frac{A}{B} = \frac{\sum_{i=1}^n a_i e_i}{\sum_{j=1}^n b_j e_j} = \frac{A \cdot \bar{B}}{B \cdot \bar{B}} = \frac{A \cdot \bar{B}}{N(B)}.$$

Таким образом, для того чтобы поделить два гиперкомплексных числа необходимо:

- определить норму знаменателя $N(B)$;
- если норма знаменателя не равна нулю, находим гиперкомплексное число, сопряженное знаменателю \bar{B} ;
- перемножаем A и \bar{B} .

Понятие нормы и сопряженного неканонического гиперкомплексного числа будет рассмотрено в третьей главе данной работы.

Пример 2.10.

Покажем деление чисел $A = a_1 \cdot E_1 + a_2 \cdot E_2$ на $B = b_1 \cdot E_1 + b_2 \cdot E_2$ в системе (2.16):

$$\begin{aligned} C &= \frac{A}{B} = \frac{A \cdot \bar{B}}{N(B)} = \frac{(a_1 \cdot E_1 + a_2 \cdot E_2) \cdot ((b_1 + b_2) \cdot E_1 - b_2 \cdot E_2)}{b_1^2 + b_1b_2 - b_2^2} \\ &= \frac{a_1 \cdot (b_1 + b_2) \cdot E_1 - a_2 \cdot b_2 \cdot E_1 + a_2 \cdot (b_1 + b_2) \cdot E_2 - b_2 \cdot (a_1 + a_2) \cdot E_2}{b_1^2 + b_1b_2 - b_2^2}. \end{aligned}$$

Пример 2.11.

Пусть заданы два числа: $A = 6E_1 + 5E_2 - 5E_3 + 12E_4$ и $B = 2E_1 + E_2 + 3E_4$, и числовая система (2.27).

$$C = \frac{A}{B} = \frac{6E_1 + 5E_2 - 5E_3 + 12E_4}{2E_1 + 1E_2 + 3E_4} = \frac{A \cdot \overline{B}}{B \cdot \overline{B}} =$$

$$= \frac{(6E_1 + 5E_2 - 5E_3 + 12E_4)(5E_1 + 1E_2 + 3E_4)}{4} = 2E_1 + 1E_2 - 5E_3 + 3E_4.$$

2.7. Использование изоморфизма неканонических ГЧС для повышения эффективности операций

Отношение изоморфизма разбивает множество гиперкомплексных числовых систем одной размерности на определенные классы, которые называют классами изоморфизма. Полученные системы, изоморфные диагональной системе, образуют один класс изоморфизма [96-98].

Как известно [1], отношение изоморфизма ГЧС - это такое взаимно однозначное отображение $f: G \rightarrow H$, что G и H две числовые системы, если для любых $a, b \in G$

$$f(a) \cdot f(b) = f(a \cdot b);$$

$$f(a) + f(b) = f(a + b). \quad (2.30)$$

Действительно, если взять для примера полученную неканоническую гиперкомплексную числовую систему, мы видим, что это свойство выполняется.

Пусть задана неканоническая гиперкомплексная система 3-й размерности и система уравнений для изоморфного перехода в диагональную систему:

E_1	E_2	E_3
E_2	$-2E_1 + 3E_3$	$-2E_1 + E_2 + 2E_3$
E_3	$-2E_1 + E_2 + 2E_3$	$-2E_1 + 3E_3$

$$E_1 = R_1 + R_2 + R_3$$

$$E_2 = -R_1 + R_2 + 2R_3$$

$$E_3 = R_1 + R_2 + 2R_3$$

Заданы два числа в диагональной системе: $A_R = 5R_1 + R_2 + R_3$, $B_R = 2R_1$.

Находим произведение этих чисел в соответствии с таблицей умножения:

$$C_R = A_R \cdot B_R = (5R_1 + R_2 + R_3)(2R_1) = 10R_1.$$

Переводим числа A_R и B_R в заданную систему:

$$A_E = E_1 - 2E_2 + 2E_3, \quad B_E = -E_2 + E_3.$$

Вычисляем произведение найденных чисел:

$$C_E = A_E \cdot B_E = (E_1 - 2E_2 + 2E_3)(-E_2 + E_3) = -5E_2 + 5E_3.$$

Система уравнений для обратного перехода в диагональную систему из заданной выглядит следующим образом:

$$R_1 = -0.5E_2 + 0.5E_3$$

$$R_2 = 2E_1 + 0.5E_2 - 1.5E_3$$

$$R_3 = -E_1 + E_3$$

Переводим число C_E в диагональную систему: $C_E \rightarrow C''_R = 10R_1$.

Полученное число C''_R соответствует произведению чисел A_R и B_R , что и требовалось показать.

То же самое с операцией сложения – можно беспрепятственно выполнять переход в изоморфную систему, выполнять операцию сложения или вычитания и осуществлять переход обратно.

Найдем сложение ранее заданных чисел A_R и B_R :

$$D_R = A_R + B_R = (5R_1 + R_2 + R_3) + (2R_1) = 7R_1 + R_2 + R_3.$$

Переводим числа A_R и B_R в систему из предыдущего примера:

$$A_E = E_1 - 2E_2 + 2E_3, \quad B_E = -E_2 + E_3.$$

Вычисляем сумму найденных чисел:

$$D_E = A_E + B_E = (E_1 - 2E_2 + 2E_3) + (-E_2 + E_3) = E_1 - 3E_2 + 3E_3.$$

Переводим число D_E в диагональную систему: $D_E \rightarrow D''_R = 7R_1 + R_2 + R_3$.

Полученное число D''_R соответствует сумме чисел A_R и B_R , что и требовалось показать.

Все вышесказанное дает нам большие возможности по оптимизации моделирования вычислительных процедур. При большом количестве итераций в алгоритме, целесообразно выполнять изоморфный переход в систему, в которой количество элементарных операций будет минимально, а затем возвращаться в исходную.

Выводы к разделу 2.

В разделе представлен обобщенный метод перечисления гиперкомплексных числовых систем – как канонических, так и неканонических. Перечисление осуществляется путем перебора сумм структурных элементов в каждой ячейке таблицы умножения. Такой метод учитывает только коэффициенты из множества $\{-1,0,1\}$ при структурных элементах, при том что количество элементов k может быть $0 \leq k \leq n$, где n размерность системы. Число таких систем заданной размерности конечно. В общем виде, с произвольными вещественными коэффициентами число гиперкомплексных числовых систем возрастает до бесконечности.

В разделе показан метод построения структур неканонических ГЧС изоморфных системе прямой суммы вещественных чисел. Для этого было использовано перечисление гиперкомплексных числовых систем методом линейных преобразований. Суть метода состоит в переборе коэффициентов при переменных в системе уравнений, с помощью которой осуществляется переход из искомой системы в диагональную, и затем получения правил умножения для полученной изоморфной системы. Алгоритм перечисления реализован и выполнен в пакете символьных вычислений MAPLE.

Усовершенствован метод построения классов изоморфизма неканонических ГЧС размерности 2. Неканоническая ГЧС общего вида со структурными константами, которые соответствуют заданным ограничениям, может быть изоморфна системе комплексных, двойных или дуальных чисел. Также показан изоморфный переход от неканонической диагональной системы к прямой сумме вещественных чисел, и, как следствие, переход от неканонической ГЧС общего вида к неканонической диагональной системе.

Рассмотрены методы перехода от бесконечномерной гиперкомплексной системы к конечномерной методами факторизации. Показана факторизация бесконечномерной ГЧС по бесконечномерным подгруппам, используя

умножение базисных элементов вида $\sigma_n \cdot \sigma_m = \frac{1}{2}(\sigma_{n+m} + \sigma_{|n-m|})$, с целью получения конечномерных гиперкомплексных систем. Полученные системы, начиная с третьей размерности, являются неканоническими. Полученные системы кратной размерности (2, 4, 6, 8...), можно повторно факторизовать и получить гиперкомплексную систему размерности в два раза меньше.

Исследованы основные операции в неканонических ГЧС. Показано, что гиперкомплексные числа сохраняют свою структуру после операций сложения и умножения. Таким образом, при переходе в изоморфную систему и выполнении операций в ней, можно сделать обратный переход в исходную систему без искажения конечного результата.

РАЗДЕЛ 3. СВОЙСТВА НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ И ОПЕРАЦИИ В НИХ

3.1. Исследование алгебраических свойств неканонических гиперкомплексных числовых систем

При использовании неканонических ГЧС в моделировании практических задач возникает необходимость определения основных свойств таких систем. Ввиду большого количества ненулевых структурных констант в таблице умножения неканонических ГЧС возникают вычислительные сложности, которые нуждаются в исследовании.

3.1.1. Единичный элемент неканонической гиперкомплексной числовой системы.

Единичный элемент гиперкомплексной числовой системы – это такое гиперкомплексное число X вида (1.1), при умножении на которое любого гиперкомплексного числа A , получается то же самое число A вида (1.1), т.е. выполняется равенство:

$$X \cdot A = A. \quad (3.1)$$

Единичный элемент может входить в базис гиперкомплексной числовой системы. В общем случае, вид единичного элемента можно определить, решив уравнение (3.1) [55].

Найдем, например, единичный элемент для неканонической числовой системы размерности 3, которая задана таблицей умножения:

$-2E_1 + E_2$	$-E_2$	$-2E_3$	(3.2)
$-E_2$	E_2	\mathbf{O}	
$-2E_3$	\mathbf{O}	$2E_1 + 2E_2$	

Допустим, что единичный элемент имеет вид:

$$\tilde{O} = x_1 \mathring{A}_1 + x_2 \mathring{A}_2 + x_3 \mathring{A}_3$$

Подставляем данное выражение в (3.1), при том, что $\dot{A} = \dot{a}_1 \dot{A}_1 + \dot{a}_2 \dot{A}_2 + \dot{a}_3 \dot{A}_3$, и получаем гиперкомплексное уравнение:

$$\begin{aligned} &(-2x_1 a_1 + 2x_3 a_3) \dot{A}_1 + (-x_1 a_1 - x_1 a_2 - x_2 a_1 + x_2 a_2 + x_2 a_3) \dot{A}_2 + \\ &+ (-2x_3 a_1 - 2x_3 a_2) \dot{A}_3 = a_1 \dot{A}_1 + a_2 \dot{A}_2 + a_3 \dot{A}_3 \end{aligned}$$

Приравняем коэффициенты при одинаковых базисных элементах. При этом получаем систему линейных алгебраических уравнений:

$$\begin{cases} -2x_1 a_1 + 2x_3 a_3 = a_1 \\ -x_1 a_1 - x_1 a_2 - x_2 a_1 + x_2 a_2 + x_3 a_3 = a_2 \\ -2x_3 a_1 - 2x_3 a_2 = a_3 \end{cases} \quad (3.3)$$

Заметим, что решения системы не должны зависеть от коэффициентов a_i числа A , так как единичный элемент зависит только от элементов базиса числовой системы.

$$\text{Решением системы будет: } x_1 = -\frac{1}{2}; x_2 = \frac{1}{2}; x_3 = 0.$$

Таким образом, единичный элемент системы, заданной таблицей (3.2), будет иметь такой вид:

$$\tilde{O} = -\frac{1}{2} \dot{A}_1 + \frac{1}{2} \dot{A}_2.$$

Выполним проверку:

$$X \cdot A = \left(-\frac{1}{2} E_1 + \frac{1}{2} E_2\right) (a_1 E_1 + a_2 E_2) = a_1 E_1 + a_2 E_2 + a_3 E_3 = A.$$

Для анализа целесообразности использования неканонических ГЧС для решения задач, необходимо дать оценку вычислительной сложности определения основных свойств таких систем. Сложность вычисления единичного элемента зависит от количества структурных элементов в ячейках таблице умножения, и, как результат, от сложности решения системы линейных уравнений вида (3.3) [39].

Так, например, для системы вида (3.2), с двумя составными ячейками, сложность вычисления единичного элемента составляет $O(n^2 + 2(n-1))$. Для неканонических гиперкомплексных числовых систем, в каждой ячейке таблиц

умножения которых присутствуют все структурные элементы, соответственно сложность вычисления будет составлять $O(n^3)$.

Для минимизации количества элементарных арифметических операций при выполнении различных вычислительных процедур целесообразно использовать неканонические ГЧС с единичным элементом в базисе.

3.1.2. Норма неканонического гиперкомплексного числа.

Нормой гиперкомплексного числа является произведение самого числа на произведение сопряженных ему чисел. Определение сопряженного рассмотрено в параграфе 3.1.3.

Как показано в [106-108], в общем виде норма гиперкомплексного числа определяется матрицей:

$$N(a) = \left\| \sum_{i=1}^n \gamma_{ij}^k a_i \right\|_{j,k=1..n} \quad (3.4)$$

где γ_{ij} – структурные константы гиперкомплексной числовой системы, а a_i – коэффициенты при базисных элементах числа.

Найдем общий вид нормы неканонического гиперкомплексного числа из системы третьей размерности, которая задана таблицей умножения:

E_1	E_2	E_3	
E_2	$2E_1 - E_3$	$-2E_1 + E_2 + 2E_3$	(3.5)
E_3	$-2E_1 + E_2 + 2E_3$	$2E_1 - E_3$	

Пусть заданы числа в системе (3.4) :

$$A = a_1 E_1 + a_2 E_2 + a_3 E_3,$$

$$B = b_1 E_1 + b_2 E_2 + b_3 E_3,$$

$$X = x_1 E_1 + x_2 E_2 + x_3 E_3.$$

Рассмотрим уравнение в заданной системе:

$$A \cdot X = B, \quad (3.6)$$

которое раскладывается, как:

$$(a_1E_1 + a_2E_2 + a_3E_3)(x_1E_1 + x_2E_2 + x_3E_3) = a_1x_1 + 2a_2x_2 - 2a_2x_3 - 2a_3x_2 + 2a_3x_3) * E_1 + (a_1x_2 + a_2x_1 + a_2x_3 + a_3x_2) * E_2 + (a_1x_3 - a_2x_2 + 2a_2x_3 + a_3x_1 + 2a_3x_2 - a_3x_3) * E_3 = b_1E_1 + b_2E_2 + a_3E_3$$

Приравняем в полученном выражении коэффициенты при структурных единицах и получим систему:

$$\begin{cases} a_1x_1 + 2a_2x_2 - 2a_2x_3 - 2a_3x_2 + 2a_3x_3 = b_1 \\ a_1x_2 + a_2x_1 + a_2x_3 + a_3x_2 = b_2 \\ a_1x_3 - a_2x_2 + 2a_2x_3 + a_3x_1 + 2a_3x_2 - a_3x_3 = b_3 \end{cases}$$

Детерминант матрицы полученной системы будет иметь вид:

$$N(A) = \begin{vmatrix} a_1 & 2a_2 - 2a_3 & -2a_2 + 2a_3 \\ a_2 & a_1 + a_3 & a_2 \\ a_3 & -a_2 + 2a_3 & a_1 + 2a_2 - a_3 \end{vmatrix} = a_1^3 + 2a_1^2a_2 - 3a_1a_3^2 - a_1a_2^2 - 2a_2^3 + 4a_1a_2a_3 + 2a_2a_3^2 + 2a_2^2a_3 - 2a_3^2 \quad (3.7)$$

что и является, по сути, нормой числа A .

В силу того, что таблица умножения неканонической гиперкомплексной числовой системы имеет большее количество базисных элементов в ячейках, уравнение (3.6) будет иметь более сложный вид.

Оценим сложность алгоритма вычисления нормы. Если принять сложность вычисления детерминанта как $O(n \cdot n!)$ [39], то сложность вычисления нормы канонического гиперкомплексного числа будет равна $O(n \cdot n! + n^2)$. Тогда для неканонической ГЧС, например, для системы вида (3.5), со всеми составными ячейками таблицы умножения, исключая первую строку и первый столбец, вычислительная сложность процедуры вычисления нормы определяется как $O(2n - 1 + (n - 1)^2 \cdot n + n \cdot n!)$ или $O(n^3 - 2n^2 + 3n - 1 + n \cdot n!)$ [109]. Для неканонической числовой системы с одной составной ячейкой в таблице умножения сложность вычисления нормы будет равна $O(n^2 + n - 1 + n \cdot n!)$. Очевидно, что для уменьшения количества

вычислительных операций целесообразно использовать неканонические гиперкомплексные системы с меньшим количеством структурных элементов в таблице.

Далее в работе будем использовать более подробные оценки асимптотической сложности вычислительных процедур, поскольку разница между сложностями алгоритмов в канонических и неканонических ГЧС не столь велика.

Покажем мультипликативность нормы для заданной системы, то есть выполнение равенства:

$$N(A * B) = N(A) * N(B)$$

В соответствии с (3.7):

$$N(A) = a_1^3 + 2a_1^2a_2 - 3a_1a_3^2 - a_1a_2^2 - 2a_2^3 + 4a_1a_2a_3 + 2a_2a_3^2 + 2a_2^2a_3 - 2a_3^3,$$

$$N(B) = b_1^3 + 2b_1^2b_2 - 3b_1b_3^2 - b_1b_2^2 - 2b_2^3 + 4b_1b_2b_3 + 2b_2b_3^2 + 2b_2^2b_3 - 2b_3^3.$$

$$\begin{aligned} N(A) * N(B) = & a_1^3(b_1^3 - 2b_2^3 - 2a_3^3 + 2b_1^2b_2 - 3b_1b_3^2 - b_1b_2^2 + 2b_2b_3^2 + 2b_3b_2^2) + \\ & + a_2^3(-2b_1^3 + 4b_2^3 + 4b_3^3 - 4b_1^2b_2 + 6b_1b_3^2 + 2a_2^3b_1b_2^2 - 4b_2b_3^2 - 4b_3b_2^2) + \\ & + a_3^3(-2b_1^3 + b_2^3 + 4b_3^3 - 4b_1^2b_2 + 6b_1b_3^2 + 2b_1b_2^2 - 4b_2b_3^2 - 4b_3b_2^2) + \\ & + b_1b_2b_3(8a_1^2a_2 - 12a_1a_3^2 + 8a_2a_3^2 + 8a_3a_2^2 + 4a_1^3 - 4a_1a_2^2 + a_2^3 - 8a_3^3) + \\ & + a_1a_2a_3(8b_1^2b_2 - 12b_1b_3^2 - 4b_1b_2^2 + 16b_1b_2b_3 + 8b_3^2b_2 + 8b_2^2b_3 + 4b_1^3 - 8b_2^3 - 8b_3^3) + \\ & + a_1^2(2a_2b_1^3 - 4a_2b_2^3 - 4a_2b_3^3 + 4a_2b_1^2b_2 - 6a_2b_1b_3^2 - 2a_2b_1b_2^2 + 4a_2b_2b_3^2 + 4a_2b_3b_2^2) + \\ & + a_3^2(-3a_1b_1^3 + 6a_1b_2^3 + 6a_3^2b_3^3 + 2a_2b_1^3 - 4a_2b_2^3 - 4a_2b_3^3 - 6a_1b_1^2b_2 + 9a_1b_1b_3^2 + \\ & + 3a_1b_1b_2^2 - 6a_1b_2b_3^2 - 6a_1b_3b_2^2 + 4a_2b_1^2b_2 - 6a_2a_1a_3^2 - 2a_2b_1b_2^2 + 4a_2b_2b_3^2 + 4a_2b_3b_2^2) + \\ & + a_2^2(-a_1b_1^3 + 2a_1b_2^3 + 2a_1b_3^3 + 2a_3b_1^3 - 4a_3b_2^3 - 4a_3b_3^3 - 2a_1b_1^2b_2 + 3a_1b_1b_3^2 + \\ & + a_1b_1b_2^2 - 2a_1b_2b_3^2 - 2a_1b_3b_2^2 + 4a_3b_1^2b_2 - 6a_3b_1b_3^2 - 2a_3b_1b_2^2 + 4a_3b_2b_3^2 + 4a_3b_3b_2^2) \end{aligned}$$

Найдем произведение чисел A и B , исходя из (3.4):

$$\begin{aligned} A * B = & (a_1b_1 + 2a_2b_2 - 2a_2b_3 - 2a_3b_2 + 2a_3b_3)E_1 + (a_1b_2 + a_2b_1 + a_2b_3 + a_3b_2)E_2 + \\ & (a_1b_3 - a_2b_2 + a_2b_3 + a_3b_1 + a_3b_2 - a_3b_3)E_3 \end{aligned}$$

Норма произведения соответственно будет равна:

$$\begin{aligned}
N(A * B) = & a_1^3(b_1^3 - 2b_2^3 - 2a_3^3 + 2b_1^2b_2 - 3b_1b_3^2 - b_1b_2^2 + 2b_2b_3^2 + 2b_3b_2^2) + a_2^3(-2b_1^3 + \\
& + 4b_2^3 + 4b_3^3 - 4b_1^2b_2 + 6b_1b_3^2 + 2a_2^3b_1b_2^2 - 4b_2b_3^2 - 4b_3b_2^2) + a_3^3(-2b_1^3 + b_2^3 + 4b_3^3 - \\
& - 4b_1^2b_2 + 6b_1b_3^2 + 2b_1b_2^2 - 4b_2b_3^2 - 4b_3b_2^2) + b_1b_2b_3(8a_1^2a_2 - 12a_1a_3^2 + 8a_2a_3^2 + 8a_3a_2^2 + \\
& + 4a_1^3 - 4a_1a_2^2 + a_2^3 - 8a_3^3) + a_1a_2a_3(8b_1^2b_2 - 12b_1b_3^2 - 4b_1b_2^2 + 16b_1b_2b_3 + 8b_3^2b_2 + \\
& + 8b_2^2b_3 + 4b_1^3 - 8b_2^3 - 8b_3^3) + a_1^2(2a_2b_1^3 - 4a_2b_2^3 - 4a_2b_3^3 + 4a_2b_1^2b_2 - 6a_2b_1b_3^2 - \\
& - 2a_2b_1b_2^2 + 4a_2b_2b_3^2 + 4a_2b_3b_2^2) + a_1^2(2a_2b_1^3 - 4a_2b_2^3 - 4a_2b_3^3 + 4a_2b_1^2b_2 - 6a_2b_1b_3^2 - \\
& - 2a_2b_1b_2^2 + 4a_2b_2b_3^2 + 4a_2b_3b_2^2) + a_3^2(-3a_1b_1^3 + 6a_1b_2^3 + 6a_3^2b_3^3 + 2a_2b_1^3 - 4a_2b_2^3 - \\
& - 4a_2b_3^3 - 6a_1b_1^2b_2 + 9a_1b_1b_3^2 + 3a_1b_1b_2^2 - 6a_1b_2b_3^2 - 6a_1b_3b_2^2 + 4a_2b_1^2b_2 - 6a_2a_1a_3^2 - \\
& - 2a_2b_1b_2^2 + 4a_2b_2b_3^2 + 4a_2b_3b_2^2) + a_2^2(-a_1b_1^3 + 2a_1b_2^3 + 2a_1b_3^3 + 2a_3b_1^3 - 4a_3b_2^3 - 4a_3b_3^3 - \\
& - 2a_1b_1^2b_2 + 3a_1b_1b_3^2 + a_1b_1b_2^2 - 2a_1b_2b_3^2 - 2a_1b_3b_2^2 + 4a_3b_1^2b_2 - 6a_3b_1b_3^2 - 2a_3b_1b_2^2 + \\
& + 4a_3b_2b_3^2 + 4a_3b_3b_2^2).
\end{aligned}$$

Таким образом производятся проверки и для других неканонических гиперкомплексных систем.

3.1.3. Сопряженные в неканонических гиперкомплексных числовых системах.

Число $\bar{A} = \sum_{i=1}^n \bar{a}_i E_i$ является сопряженным гиперкомплексному числу

(1.1) если:

$$A \cdot \bar{A} = X,$$

где X - единичной элемент выбранной ГЧС.

Как уже было указано, норма гиперкомплексного числа определяется матрицей (3.4). В свою очередь, для сопряженных должно выполняться равенство:

$$a \cdot a_{c_1} \cdot \dots \cdot a_{c_{n-1}} = N(a) \cdot X, \quad (3.8)$$

где X - соответствует единичному элементу заданной гиперкомплексной числовой системы. Допустим, что

$$a_{ck} = x_{1k} E_1 + x_{2k} E_2 + \dots + x_{nk} E_n, k=1, \dots, n-1. \quad (3.9)$$

Если подставить (3.9) в (3.8) и приравнять выражения при одинаковых базисных элементах, получим систему из $(n - 1)$ квадратичных уравнений от $n(n-1)$ неизвестных [77-81], решение которой может представлять значительные трудности. Если же система не имеет решения в действительных числах, то можно найти произведение сопряженных, которое в основном и используется для вычислений:

$$a_{c_1} \cdot a_{c_2} \cdot \dots \cdot a_{c_{n-1}} = \bar{a} = x_1 E_1 + x_2 E_2 + \dots + x_n E_n, \quad (3.10)$$

Найдем произведение сопряженных в неканонической числовой системе (3.5). Норма числа такой числовой системы имеет вид:

$$N(A) = a_1^3 + 2a_1^2 a_2 - 3a_1 a_3^2 - a_1 a_2^2 - 2a_2^3 + 4a_1 a_2 a_3 + 2a_2^2 a_3 - 2a_3^2.$$

С учетом (3.10) и (3.8) получаем систему:

$$\left\{ \begin{array}{l} a_1 x_1 + 2a_2 x_2 - 2a_2 x_3 - 2a_3 x_2 + 2a_3 x_3 = \\ = a_1^3 + 2a_1^2 a_2 - 3a_1 a_3^2 - a_1 a_2^2 - 2a_2^3 + 4a_1 a_2 a_3 + 2a_2^2 a_3 - 2a_3^2 \\ a_1 x_2 + a_2 x_1 + a_2 x_3 + a_3 x_2 = 0 \\ a_1 x_3 - a_2 x_2 + a_2 x_3 + a_3 x_1 + a_3 x_2 - a_3 x_3 = 0 \end{array} \right. \quad (3.11)$$

Решением системы (3.11), т.е. произведением сопряженных будет:

$$a_{c_1} * a_{c_2} = \bar{a} = (a_1^2 + 2a_1 a_2 - a_3^2 + a_2^2) E_1 + \\ + (-a_2^2 - a_1 a_2 + 2a_2 a_3) E_2 + (-a_2^2 + 2a_2 a_3 - a_1 a_3 - a_3^2) E_3$$

Как видим, для неканонической гиперкомплексной числовой системы с единицей в базисе процедура нахождения произведения сопряженных практически не отличается от канонических ГЧС. Тем не менее, сопряженные в неканонических ГЧС, как правило, имеют более сложный вид, что обусловлено большим количеством структурных единиц в ячейках таблиц умножения неканонических гиперкомплексных числовых систем.

Рассмотрим произведение сопряженных в неканонической гиперкомплексной числовой системе (3.2), единичный элемент и норма которой имеет вид:

$$X = -\frac{1}{2} * E_1 + \frac{1}{2} * E_2, \quad (3.12)$$

$$N(A) = -4a_1^3 + 4a_1^2a_2 + 4a_1a_3^2 - 4a_2a_3^2 \quad (3.13)$$

Система уравнений соответственно будет иметь вид:

$$\begin{cases} -2x_1a_1 + 2x_3a_3 = -\frac{1}{2}(-4a_1^3 + 4a_1^2a_2 + 4a_1a_3^2 - 4a_2a_3^2) \\ -x_1a_1 - x_1a_2 - x_2a_1 + x_2a_2 + x_3a_3 = \frac{1}{2}(-4a_1^3 + 4a_1^2a_2 + 4a_1a_3^2 - 4a_2a_3^2) \\ -2x_3a_1 - 2x_3a_1 = 0 \end{cases}$$

или

$$\begin{cases} -x_1a_1 + x_3a_3 = a_1^3 - a_1^2a_2 - a_1a_3^2 + a_2a_3^2 \\ -x_1a_1 - x_1a_2 - x_2a_1 + x_2a_2 + x_3a_3 = -2a_1^3 + 2a_1^2a_2 + 2a_1a_3^2 - 2a_2a_3^2 \\ -2x_3a_1 - 2x_3a_1 = 0 \end{cases} \quad (3.14)$$

Решением системы (3.14) будет:

$$\begin{aligned} x_1 &= \frac{a_1(a_1^3 - a_1^2a_2 - a_1a_3^2 + a_2a_3^2)}{a_1^2 + a_3^2}; \\ x_2 &= -\frac{-3a_1^4 - a_1^3a_2 - a_1a_2a_3^2 + 3a_3^4}{a_1^2 + a_3^2}; \\ x_3 &= \frac{a_3(a_1^3 - a_1^2a_2 - a_1a_3^2 + a_2a_3^2)}{a_1^2 + a_3^2}. \end{aligned}$$

Соответственно произведение сопряженных будет иметь вид:

$$\begin{aligned} \bar{a} &= \frac{a_1(a_1^3 - a_1^2a_2 - a_1a_3^2 + a_2a_3^2)}{a_1^2 + a_3^2} E_1 - \\ &- \frac{-3a_1^4 - a_1^3a_2 - a_1a_2a_3^2 + 3a_3^4}{a_1^2 + a_3^2} E_2 + \frac{a_3(a_1^3 - a_1^2a_2 - a_1a_3^2 + a_2a_3^2)}{a_1^2 + a_3^2} E_3. \end{aligned}$$

Вид полученного произведения сопряженных для неканонической ГЧС без единичного элемента в базисе довольно сложный, и он напрямую зависит от вида единичного элемента. Сложность процедуры вычисления сопряженного соизмерима со сложностью процедуры вычисления единичного элемента [96]. Для упрощения вычислений при моделировании задач с использованием

неканонических гиперкомплексных числовых систем целесообразно использовать системы с единицей в базисе.

3.1.4. Делители нуля в неканонических гиперкомплексных числовых системах.

Делителем нуля в неканонической гиперкомплексной числовой системе является число a , обладающее такими свойствами [94]:

- это число отлично от нуля: $a \neq 0$;
- существует такое отличное от нуля число b с этой же гиперкомплексной числовой системы Q , что произведение чисел a и b равняется нулю: $a \cdot b = 0$; $a, b \neq 0$; $a, b \in Q$.
- если a - делитель нуля, $\alpha \in \mathbf{R}$, то и αa также является делителем нуля.

В соответствии с теоремой Фробениуса [21], поле вещественных чисел и поле комплексных чисел являются единственными конечномерными ассоциативно-коммутативными алгебрами без делителей нуля, тело кватернионов является единственной конечномерной ассоциативной, но не коммутативной алгеброй без делителей нуля, алгебра Кэли является единственной конечномерной альтернативной, но не ассоциативной алгеброй без делителей нуля.

Очевидно [108], что норма делителя нуля равна нулю:

$$N(a \cdot b) = 0,$$

Таким образом, чтобы найти делители нуля необходимо решить уравнение:

$$\left\| \sum_{i=1}^n \gamma_{ij}^k a_i \right\| = 0.$$

Рассмотрим определение делителей нуля для неканонической ГЧС размерности 2.

E_1	E_2
E_2	$-3E_1 + 4E_2$

(3.14)

Уравнение для этой числовой системы будет равно:

$$N(A) = a_1^2 + 4a_1a_2 + 3a_2^2 = 0.$$

Соответственно, делители нуля для системы (3.14) имеют такой вид, что:

$$a_1 = -a_2 \text{ или } a_1 = -3a_2.$$

Определим делители нуля для неканонической гиперкомплексной числовой системы (3.5). Уравнение для данной системы будет иметь вид:

$$N(A) = a_1^3 + 2a_1^2a_2 - 3a_1a_3^2 - a_1a_2^2 - 2a_2^3 + 4a_1a_2a_3 + 2a_2^2a_3 - 2a_3 = 0.$$

Делитель нуля для системы (3.5) будет иметь такой вид, что:

$$a_1^2 = \frac{-a_1^3 + 3a_1a_3^2 + a_1a_2^2 + 2a_2^3 - 4a_1a_2a_3 - 2a_2^2a_3 + 2a_3}{2a_2}.$$

С возрастанием количества структурных элементов в таблице умножения неканонической ГЧС, возрастает сложность вида нормы числа такой системы, а, соответственно, и вычисление делителей нуля. Как видим, для неканонических ГЧС более высоких размерностей количество операций по проверке коэффициентов a_1, a_2, \dots, a_n соизмеримо с количеством операций по вычислению нормы неканонического гиперкомплексного числа. Поэтому при проведении вычислений, в которых требуется проверка на делители нуля, целесообразно вычислять норму и проверять, равна ли она нулю.

Определим делители нуля для неканонических ГЧС, изоморфных комплексным числам и кватернионам.

Проанализируем неканонические гиперкомплексные числовые системы, изоморфные комплексным числам. Приведем пример одной из них:

E_1	E_2
E_2	$-32E_1 - 8E_2$

(3.15)

Норма числа A такой системы будет иметь вид:

$$N(A) = \begin{vmatrix} a_1 & -32a_2 \\ a_2 & a_1 - 8a_2 \end{vmatrix} = a_1^2 - 8a_1a_2 + 32a_2^2 = (a_1 - 4a_2)^2 + 16a_2^2 \quad (3.16)$$

Очевидно, что норма вида (3.16) будет равняться нулю только тогда, когда число A будет равно нулю.

В ходе исследований были проанализированы 47 неканонических ГЧС, изоморфных системе комплексных чисел, которые были построены с помощью метода, описанного в подразделе 2.2 и представлены в Приложении Г.

Можно утверждать, что ни в одной из этих систем нет делителей нуля. Нормы чисел этих систем равны нулю только тогда, когда само число равно нулю, и имеют вид:

$$N(A) = (a_1 \pm Ca_2)^2 + Da_2^2,$$

где C и D вещественные коэффициенты при структурных элементах в таблице умножения системы.

В случае с неканоническими ГЧС, изоморфные кватернионам, норма будет выглядеть немного сложнее. Рассмотрим одну из таких систем:

E_1	E_2	E_3	E_4
E_2	$-4E_1 + 4E_4$	$-2E_3$	$-E_4$
E_3	$-2E_3$	$-2E_4$	$2E_3$
E_4	$-2E_4$	$2E_3$	$2E_4$

(3.17)

Норма числа A в такой системе будет равна:

$$N(A) \begin{vmatrix} a_1 & -4a_2 & 0 & 0 \\ a_2 & a_1 & 0 & 0 \\ a_3 & -2a_3 & a_1 - 2a_2 + 2a_4 & 2a_3 \\ a_4 & 4a_2 - 2a_4 & -2a_3 & a_1 - 2a_2 + 2a_4 \end{vmatrix} =$$

$$= a_1^4 - 4a_1^3a_2 + 4a_1^3a_4 + 8a_1^2a_2^2 - 8a_1^2a_2a_4 + 4a_1^2a_4^2 + 4a_1^2a_3^2 -$$

$$- 16a_2^3a_1 + 16a_2^2a_1a_4 + 16a_2^4 - 32a_2^3a_4 + 16a_2^2a_4^2 + 16a_2^2a_3^2$$

или

$$N(A) = a_1^2(-2a_2 + 2a_4 + a_1)^2 + a_2^2(2a_1 + 4a_4 - 4a_2)^2 + 4a_1^2a_3^2 + 16a_2^2a_3^2. \quad (3.18)$$

Очевидно, что норма числа (3.18) системы (3.17) будет равняться нулю только тогда, когда число A будет равно нулю.

Рассмотрим более сложную неканоническую ГЧС, изоморфную кватернионам:

E_1	E_2	E_3	E_4
E_2	$-2E_2 + 2E_3 - 4E_4$	$-4E_1 - 2E_2 - 2E_3$	$-E_3$
E_3	$-4E_1 - 2E_2 - 2E_3$	$2E_2 - 2E_3 + 4E_4$	E_2
E_4	$-E_3$	E_2	$-E_1$

(3.19)

Норма числа A в системе (3.19) соответственно будет равна:

$$N(A) \begin{vmatrix} a_1 & -4a_3 & -4a_2 & -a_4 \\ a_2 & a_1 - 2a_2 - 2a_3 & -2a_2 + 2a_3 + a_4 & a_3 \\ a_3 & 2a_2 - 2a_3 - a_4 & a_1 - 2a_2 + 2a_3 & -2a_2 \\ a_4 & -4a_2 & 4a_3 & a_1 \end{vmatrix}$$

или

$$\begin{aligned} N(A) = & a_1^2(-2a_2 + a_4 - 2a_3 + a_1)^2 + 2a_2^2(-2a_1 - 2a_4 + 2a_2 - \\ & - 2a_1)^2 + a_3^2(-4a_2 + 2a_4 + 4a_3 + 2a_1)^2 + a_4^2(-2a_1 + a_2 + a_2)^2 + \\ & + a_4^2(-2a_2 + a_4 - 2a_3)^2 + 2a_2^2(2a_2 + 2a_3)^2 + \\ & + 2a_1(4a_3a_4 - 2a_2^2 - a_4^2 - a_1a_4 + 4a_2a_3) + 4a_2^2(-a_4^2 - 8a_1a_3) + \\ & + 8a_3^2(-4a_1a_3 + 4a_2a_3 - 3a_1a_4) + a_4^2(-10a_2a_3 - a_1^2 - a_2^2 - a_3^2) \end{aligned} \quad (3.20)$$

Исходя из вида нормы, сложно сказать, без дополнительного анализа, есть ли у системы (3.19) делители нуля. Поэтому, приравнивая выражение (3.20) к нулю, находим чему равны коэффициенты a_1, a_2, a_3, a_4 :

$$a_1 = 2a_2 \pm (2a_3 + a_4)i, \quad a_1 = 2a_3 \pm (-2a_2 + a_4)i$$

$$a_2 = a_1 \pm (2a_3 + a_4)i, \quad a_2 = a_4 \pm (2a_3 - a_1)i$$

$$a_3 = -a_4 \pm (2a_2 - a_1)i, \quad a_3 = a_1 \pm (-2a_2 + a_4)i$$

$$a_4 = -2a_3 \pm (2a_2 - a_1)i, \quad a_4 = 2a_2 \pm (2a_3 - a_1)i$$

Решения в вещественных числах нет, поэтому можно утверждать, что для системы (3.19) не существует делителей нуля.

В ходе исследования были проанализированы 35 числовых систем 4-й размерности изоморфных кватернионам, построенных с помощью метода, описанного в подразделе 2.2. У всех этих систем не найдены делители нуля.

3.2. Модулярная арифметика в неканонических гиперкомплексных числовых системах

3.2.1. Общий подход к вычислению вычетов в гиперкомплексных числовых системах.

Для решения задач криптографии с применением ГЧС, необходимо построить общий подход к вычислению наименьших вычетов. Наименьшие вычеты в гиперкомплексных числах определяются исходя из таблицы умножения ГЧС и вида сопряженных.

Пусть $\bar{b} = b_{11}e_1 + b_{12}e_2 + \dots + b_{1n}e_n$ - гиперкомплексное число, которое равно произведению сопряженных числа b . Обозначим норму b как $N(b) = B$. Тогда, в соответствии с (2.6) справедлива такая формула [60-62]:

$$\frac{a}{b} = \frac{a \cdot \bar{b}}{B} = \frac{u}{B} = \frac{u_1}{B}e_1 + \frac{u_2}{B}e_2 + \dots + \frac{u_n}{B}e_n, \quad (3.21)$$

где u_1, u_2, \dots, u_n - коэффициенты при единицах кольца числа w .

Определим величины w_1, w_2, \dots, w_n как $u_1 \equiv w_1 \pmod{B}$, $u_2 \equiv w_2 \pmod{B}$, ..., $u_n \equiv w_n \pmod{B}$. Тогда наименьший вычет будет равен величине:

$$r = r_1e_1 + r_2e_2 + \dots + r_n e_n = \frac{w \cdot b}{B}. \quad (3.22)$$

Докажем данное утверждение для неканонической ГЧС вида (3.14). Пусть дано число $A = a_1E_1 + a_2E_2$, и модуль $B = b_1E_1 + b_2E_2$. Сопряженное числа b будет иметь вид:

$$\bar{B} = (b_1 + 4b_2)E_1 - b_2E_2.$$

Тогда деление числа a на b будет выглядеть следующим образом:

$$\frac{A}{B} = \frac{\overline{AB}}{N(B)} = \frac{a_1(b_1 + 4b_2) + 3a_2b_2}{b_1^2 + 4b_1b_2 + 3b_2^2} E_1 + \frac{-a_1b_2 + a_2b_1}{b_1^2 + 4b_1b_2 + 3b_2^2} E_2$$

Задав вычет $|\bullet|_N$ по вещественному модулю $N = N(B)$, находим однозначное разложение

$$\begin{aligned} a_1(b_1 + 4b_2) + 3a_2b_2 &= | a_1(b_1 + 4b_2) + 3a_2b_2 |_N + b_1N \\ -a_1b_2 + a_2b_1 &= | -a_1b_2 + a_2b_1 |_N + b_2N \end{aligned}$$

Поэтому получим разложение

$$\begin{aligned} r &= (| a_1(b_1 + 4b_2) + 3a_2b_2 |_N \cdot E_1 + \\ &| -a_1b_2 + a_2b_1 |_N \cdot E_2) \frac{b}{N(b)} + (b_1E_1 + b_2E_2), \end{aligned}$$

которое тоже определено однозначно.

Таким образом, если обозначить $(a_1E_1 + a_2E_2)_b$ - остаток от деления числа $a = a_1E_1 + a_2E_2$ на $b = b_1E_1 + b_2E_2$, то справедлива формула

$$\begin{aligned} (a_1E_1 + a_2E_2)_b &= (| a_1(b_1 + 4b_2) + 3a_2b_2 |_N * E_1 + | -a_1b_2 + a_2b_1 |_N * E_2) \frac{b}{N(B)} \\ &= \frac{(w_1E_1 + w_2E_2)(b_1E_1 + b_2E_2)}{N(B)} \end{aligned}$$

Отсюда наименьший вычет для неканонического гиперкомплексного числа системы (3.14) будет равен :

$$r = r_1E_1 + r_2E_2 = \frac{(w_1b_1 - 3w_2b_2) * E_1 + (w_1b_2 + w_2b_1 + 4w_2b_2) * E_2}{N(B)}$$

Рассмотрим пример:

$$a = -10E_1 + 11E_2,$$

$$b = 3E_1 + 4E_2.$$

Тогда

$$\frac{-10E_1 + 11E_2}{3E_1 + 4E_2} = \frac{-58}{105} E_1 + \frac{73}{105} E_2$$

$$w_1 = -58 \bmod(105) \equiv 47,$$

$$w_2 = 73 \bmod(105) \equiv 73,$$

$$\Rightarrow r = -7E_1 + 15E_2.$$

Таким образом, общая формула (3.21) доказывается для каждой исследуемой числовой системы.

3.2.2. Особенности вычисления вычетов в неканонических гиперкомплексных числовых системах.

В неканонических гиперкомплексных числовых системах вычисление наименьших вычетов несколько отличается от канонических гиперкомплексных числовых систем. Как уже было сказано, в канонических гиперкомплексных числовых системах в ячейках таблицы умножения присутствует только один структурный элемент с коэффициентами $\{1, 0, -1\}$. Неканонические числовые системы имеют более сложную структуру, и, соответственно, более сложную процедуру вычисления наименьших вычетов.

Первый вопрос, который необходимо решить при использовании наименьших вычетов в вычислениях, это модуль отрицательного числа в выражении (3.21). То есть, вычисление $u_1 \equiv w_1 \pmod{B}$, ..., $u_n \equiv w_n \pmod{B}$, при $w_i < 0$. Как правило, вычет отрицательного числа по какому-либо модулю вычисляют как наименьший положительный остаток.

Рассмотрим пример. Найдем наименьший вычет для неканонического гиперкомплексного числа $A = -12E_1 - 30E_3$ по модулю $B = -21E_1 + 17E_3$ из системы, заданной таблицей:

E_1	E_2	E_3	(3.23)
E_2	$E_1 - 2E_2 - E_3$	$E_1 + E_2 - E_3$	
E_3	$E_1 + E_2 - E_3$	$-2E_1 + 3E_3$	

$$\frac{A}{B} = \frac{-12E_1 - 30E_3}{-21E_1 + 17E_3} = \frac{5520E_1 - 3336E_3}{208}, \quad (3.24)$$

$$5520 \equiv 112 \pmod{208}, \quad 0 \equiv 0 \pmod{208}, \quad -3336 \equiv 200 \pmod{208},$$

$$r = \frac{(112E_1 + 200E_3)(-21E_1 + 17E_3)}{208} = -44E_1 + 38E_3.$$

В тоже время, наименьший вычет гиперкомплексного числа – это вычет с наименьшей нормой. При этом норма вычета должна быть меньше, чем сам модуль. В вышеуказанном примере, норма вычета равняется $N(r) = 1152$, а модуля $N(B) = 208$. Для канонических гиперкомплексных числовых систем это может и не влиять исход вычислений, так как при итеративном выполнении, например, алгоритма Евклида, значения корректируются за счет простого вида таблицы умножения и коэффициентов в ней равных нулю или единице. Для неканонических гиперкомплексных числовых систем итеративные вычисления с отклонениями такого рода могут привести к увеличению значений вычетов до бесконечности.

Логично предположить, что в таком случае, вычет отрицательного числа лучше вычислять как:

$$\begin{cases} w_i^- \pmod{B}, w_i^- < 0, |w_i^-| < w_i^+ \\ w_i^+ \pmod{B}, w_i^+ \geq 0, |w_i^-| \geq w_i^+ \end{cases} \quad (3.25)$$

Определим теперь вычеты для полученного выражения (3.24):

$$5520 \equiv 112 \pmod{208}, \quad 0 \equiv 0 \pmod{208}, \quad -3336 \equiv -8 \pmod{208},$$

$$r = \frac{(112E_1 - 8E_3)(-21E_1 + 17E_3)}{208} = \frac{-2080E_1 + 1664E_3}{208} = -10E_1 + 8E_3,$$

$$N(r) = 24.$$

Как видим, норма наименьшего вычета меньше чем норма модуля, что обеспечивает сходимость вычислительных процедур.

Тем не менее, как уже было сказано, неканонические гиперкомплексные числовые системы имеют более сложную структуру, и выражение (3.25) может быть применимо не только к поиску остатков от отрицательного числа. Рассмотрим вычисление вычета, с учетом (3.25) в неканонической гиперкомплексной числовой системы 2-й размерности:

E_1	E_2
E_2	$-5E_1 + 4E_2$

(3.26)

$$\frac{A}{B} = \frac{-7E_1 + 3E_2}{2E_1 + E_2} = \frac{(-7E_1 + 3E_2)(6E_1 - E_2)}{17} = \frac{-27E_1 + 13E_2}{17},$$

$$-27 \equiv 7(\text{mod } 17), \quad 13 \equiv 13(\text{mod } 17),$$

$$r = \frac{(7E_1 + 13E_2)(2E_1 + E_2)}{17} = -3E_1 + 5E_2,$$

Норма вычета равна $N(r) = 74$, при норме модуля $N(B) = 17$. В то же время, если принять во внимание (3.25) для $u_i > 0$ из (3.21), то

$$-27 \equiv 7(\text{mod } 17), \quad 13 \equiv -4(\text{mod } 17),$$

$$r = \frac{(7E_1 - 4E_2)(2E_1 + E_2)}{17} = \frac{34E_1 - 17E_2}{17} = 2E_1 - E_2,$$

$$N(r) = 1.$$

Таким образом, при вычислении вычетов для неканонических ГЧС целесообразно использовать выражение (3.25) для всех u_i из (3.21). При такой реализации алгоритма, обеспечивается сходимость в алгоритме Евклида, который будет описан в следующем параграфе.

В неканонических гиперкомплексных числовых системах, в которых не выполняется свойство мультипликативности нормы, невозможно вычисление вычетов. Так, например для системы (3.27), мы получим дробные величины при вычислении вычетов:

E_1	E_2	E_3
E_2	$-3E_2 + E_3$	$-E_2$
E_3	$-E_2$	$-3E_3$

(3.27)

$$\frac{A}{B} = \frac{7E_1 + 3E_2 - 4E_3}{2E_1 + E_2 + E_3} = \frac{(7E_1 + 3E_2 - 4E_3)(E_1 - E_2 + 3E_3)}{2} = \frac{7E_1 - 8E_2 + 38E_3}{2}$$

$$7 \equiv 1(\text{mod } 2), \quad -8 \equiv 0(\text{mod } 2), \quad 38 \equiv 0(\text{mod } 2),$$

$$r = \frac{(E_1)(2E_1 + E_2 + E_3)}{2} = \frac{2E_1 + E_2 + E_3}{2} = E_1 + 0.5E_2 + 0.5E_3.$$

Очевидно, что дальнейшие вычисления, связанные с вычетами в такой системе проводить нецелесообразно, так как вычетов с дробными коэффициентами не существует.

3.3. Процедура, реализующая алгоритм Евклида для неканонических гиперкомплексных числовых системах

Из определения евклидова кольца следует, что для любых элементов $a, b \in R$, где $b \neq 0$, в кольце вещественных чисел можно так подобрать элементы q и r , что $a = bq + r$, причем или $r = 0$, или же $n(r) < n(b)$. Тогда для отыскания наибольшего общего делителя применяется алгоритм Евклида. Как известно [60-62], возможна реализация алгоритма Евклида в области канонических гиперкомплексных чисел. Рассмотрим реализацию алгоритма в неканонических гиперкомплексных числах.

Учитывая то, что в дальнейшем будет рассмотрен алгоритм Евклида для неканонических ГЧС, восстановим суть алгоритма в первоначальном виде для вещественных чисел.

Пусть a и b - положительные целые. Находим ряд равенств :

$$\left. \begin{array}{l} a = bq_1 + r_2, 0 < r_2 < b, \\ b = r_2q_2 + r_3, 0 < r_3 < r_2, \\ \dots\dots\dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_n. \end{array} \right\}$$

заканчивающийся тогда, когда получаем некоторое значение $r_{n+1} = 0$. Последнее неизбежно, так как ряд b, r_2, r_3, \dots как ряд убывающих чисел не может содержать более чем b положительных чисел.

Общие делители чисел a и b одинаковы с общими делителями чисел b и r_2 , далее одинаковы с общими делителями чисел r_2 и r_3 , чисел r_3 и r_4 и т.д., и, наконец, с делителем числа r_n . Одновременно с этим имеем

$$(a, b) = (b, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n.$$

Следовательно, наибольший общий делитель равен r_n . Для взаимно простых чисел $r_n = 1$ [60-62].

Из теории чисел известно, что для любых взаимно простых a и b найдутся такие x и y , что $ax + by = 1$. При чем $ax = 1(\text{mod } b)$ и $by = 1(\text{mod } a)$.

Предположим, $a > b$. Тогда мы можем решить уравнения:

$$\begin{aligned} ax + by &= a, \\ ax + by &= b. \end{aligned}$$

Первое уравнение имеет решение $x_0 = 1, y_0 = 0$, второе уравнение имеет решение $x_1 = 0, y_1 = 1$, где единица является единичным элементом для гиперкомплексной числовой системы.

Выполняя последовательно шаги алгоритма Евклида, получим систему уравнений для вычисления $x_i, y_i, x_{i-1}, y_{i-1}$:

$$\begin{aligned} r_{i-1}x_{i-1} + r_i y_{i-1} &= r_{i-1}, \\ r_{i-1}x_i + r_i y_i &= r_i. \end{aligned} \quad i = 1 \dots n \quad (3.28)$$

Инициализируем начальные значения : $r_0 = a, r_1 = b$.

Далее выразим r_{i+1} :

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i = r_{i-1}x_{i-1} + r_i y_{i-1} - q_i (r_{i-1}x_i + r_i y_i) \\ r_{i+1} &= r_{i-1}(x_{i-1} - q_i x_i) + r_i(y_{i-1} - q_i y_i) = r_{i-1}x_{i+1} + r_i y_{i+1} \end{aligned} \quad (3.29)$$

Следовательно,

$$\begin{aligned} x_{i+1} &= x_{i-1} - q_i x_i, \\ y_{i+1} &= y_{i-1} - q_i y_i. \end{aligned} \quad (3.30)$$

Поскольку $r_{n+1} = 0$, и для взаимно простых чисел $r_n = 1$, искомые переменные будут равняться x_n и y_n .

Отличие алгоритма Евклида с элементами A и B в виде неканонических гиперкомплексных чисел состоит в том, что у взаимно простых гиперкомплексных чисел сохраняется соотношение $ax + by = E$, где E – единичный элемент неканонической ГЧС. Начальные значения алгоритма соответственно равны $x_0 = E$, $y_0 = E$. Также для неканонических гиперкомплексных чисел достаточно, чтобы $N(r_n) = 1$. Тогда на последнем шаге алгоритма x_n и y_n делится на r_n , и результатом будут искомые x и y .

Рассмотрим пример. Пусть задана неканоническая ГЧС с таблицей умножения:

E_1	E_2
E_2	$-5E_1 + 4E_2$

(3.31)

Пусть $AX + BY = E_1$, где $A = -40E_1 + 11E_2$ и $B = E_1 - 2E_2$. Найдём X и Y для данного уравнения.

Инициализируем начальные значения:

$$\begin{aligned} r_0 &= -40E_1 + 11E_2, & x_0 &= E_1, & y_0 &= 0, \\ r_1 &= E_1 - 2E_2, & x_1 &= 0, & y_1 &= E_1. \end{aligned}$$

Выполняем последовательно шаги алгоритма:

$$1) \frac{r_0}{r_1} = \frac{-40E_1 + 11E_2}{E_1 - 2E_2} = \frac{76}{5}E_1 + \frac{-69}{5}E_2$$

$$76 \bmod(5) \equiv 1, \quad -69 \bmod(5) \equiv -4,$$

$$\Rightarrow r_2 = \frac{(E_1 - 4E_2)(E_1 - 2E_2)}{5} = -3E_1 + 2E_2,$$

$$q_1 = \frac{(-40E_1 + 11E_2) - (-3E_1 + 2E_2)}{E_1 - 2E_2} = 15E_1 - 13E_2,$$

$$x_2 = x_0 - q_1x_1 = E_1 - (15E_1 - 13E_2) \cdot 0 = E_1,$$

$$y_2 = y_0 - q_1y_1 = 0 - (15E_1 - 13E_2)E_1 = -15E_1 + 13E_2.$$

$$2) \frac{r_1}{r_2} = \frac{E_1 - 2E_2}{-3E_1 + 2E_2} = \frac{-7}{5}E_1 + \frac{4}{5}E_2,$$

$$-7(5) \equiv -2, \quad 4 \bmod(5) \equiv 4,$$

$$\Rightarrow r_3 = \frac{(-2E_1 + 4E_2)(-3E_1 + 2E_2)}{5} = -2E_1,$$

$$q_2 = \frac{(E_1 - 2E_2) - (-2E_1)}{E_1 - 2E_2} = -E_1,$$

$$x_3 = x_1 - q_2 * x_2 = 0 - (-E_1) * E_1 = 2E_1,$$

$$y_3 = y_1 - q_2 * y_2 = E_1 - (-E_1)(-15E_1 + 13E_2) = -14E_1 + 13E_2.$$

$$3) \frac{r_2}{r_3} = \frac{-3E_1 + 2E_2}{-2E_1} = \frac{6}{4}E_1 + \frac{-4}{4}E_2,$$

$$6(4) \equiv 2, \quad 4 \bmod(4) \equiv 0,$$

$$\Rightarrow r_4 = \frac{(2E_1)(-2E_1)}{4} = \frac{-4E_1}{4} = -E_1,$$

$$q_3 = \frac{(-2E_1) - (-E_1)}{E_1 - 2E_2} = E_1 - E_2,$$

$$x_4 = x_2 - q_3 x_3 = E_1 - (E_1 - E_2) \cdot 2E_1 = E_2,$$

$$y_4 = y_2 - q_3 y_3 = -15E_1 + 13E_2 - (E_1 - E_2)(-14E_1 + 13E_2) = -27E_1 + 12E_2$$

$$4) \frac{r_3}{r_4} = \frac{-2E_1}{-E_1} = 2E_1,$$

$$\Rightarrow r_5 = 0,$$

$$q_4 = 2E_1,$$

$$x_5 = x_3 - q_4 x_4 = 2E_1 - (2E_1) \cdot E_2 = E_1 - 2E_2,$$

$$y_5 = y_3 - q_4 y_4 = -14E_1 + 13E_2 - (2E_1)(-27E_1 + 12E_2) = 40E_1 - 11E_2.$$

Поскольку $r_4 = -E_1$, то получаем

$$X = x_4 / (-E_1) = \frac{E_2}{-E_1} = -E_1,$$

$$Y = y_5 / (-E_1) = \frac{-27E_1 + 12E_2}{-E_1} = 27E_1 - 12E_2.$$

Производим проверку:

$$AX + BY = (-40E_1 + 11E_2)(-E_1) + (E_1 - 2E_2)(-27E_1 + 12E_2) = E_1.$$

Таким образом, отличие реализации и выполнения алгоритма Евклида для неканонических систем состоит в степени вычислительной сложности, которая, как и все арифметические характеристики, напрямую зависит от сложности таблицы умножения выбранной числовой системы. Также, при моделировании аналога алгоритма Евклида для неканонических гиперкомплексных чисел необходимо отслеживать появление делителей нуля. Числовая система (3.26), которая использовалась для предыдущего примера, изоморфна комплексным числам и, как описывалось ранее, не имеет делителей нуля. Если же для моделирования алгоритма используется, например, неканоническая ГЧС, изоморфная двойным числам, то появление делителей нуля среди наименьших вычетов делает невозможным дальнейшие вычисления и поиск неизвестных X и Y .

Как уже было сказано в предыдущем подразделе, сходимость в выполнении алгоритма Евклида в неканонических ГЧС обеспечивается, если система удовлетворяет требованию мультиприкативности нормы.

Рассмотрим пример. Пусть задана неканоническая ГЧС таблицей умножения (3.27).

E_1	E_2	(3.27)
E_2	$8E_2$	

Числа $A = -6E_1 + 2E_2$ и $B = E_1 + 3E_2$ взаимно простые. Найдем решение уравнения $AX + BY = E_1$:

$$\frac{r_0}{r_1} = \frac{-6E_1 + 2E_2}{E_1 + 3E_2} = \frac{-150}{25}E_1 + \frac{16}{25}E_2,$$

$$-150 \bmod(25) \equiv 0, \quad 16 \bmod(25) \equiv 16,$$

$$\Rightarrow r_2 = \frac{(16E_2)(E_1 + 3E_2)}{25} = 16E_2.$$

Норма $N(r_2) = 0$, поэтому дальнейшие шаги алгоритма пройти невозможно. Более того, уравнения (3.28) для $r_2 = 16E_2$ не будут выполняться,

что говорит о неприменимости алгоритма Евклида для поиска неизвестных X и Y .

Можно сделать вывод, что для моделирования аналога алгоритма Евклида для неканонических гиперкомплексных числовых систем, рациональнее будет использовать числовые системы, которые не имеют делителей нуля. Если же возникла необходимость использования других неканонических гиперкомплексных числовых систем, то целесообразно дополнять алгоритм соответствующими проверками на корректное выполнение всех действий данной вычислительной процедуры.

Выводы по разделу 3

Рассмотрено построение единичного элемента неканонической гиперкомплексной числовой системы. Показана вычислительная сложность данной процедуры для неканонических ГЧС в общем виде. Можно утверждать, что для повышения эффективности вычислительных процедур целесообразно использовать неканонические гиперкомплексные числовые системы с единичным элементом в базисе.

Рассмотрено построение нормы неканонической ГЧС, показана вычислительная сложность данной процедуры для неканонических гиперкомплексных числовых систем различного вида. Для минимизации вычислительных операций нужно использовать неканонические гиперкомплексные числовые системы с наименьшим количеством структурных элементов в таблице умножения.

Модифицирован метод проверки свойства мультипликативности нормы.

Промоделировано определение сопряженных для неканонических гиперкомплексных числовых систем. Вычислительная сложность алгоритма соизмерима со сложностью определения единичного элемента. Для систем с единицей в базисе вычислительная сложность построения сопряженных для неканонических ГЧС не отличается от построения сопряженных в канонических ГЧС.

Рассмотрено определение делителей нуля в неканонических ГЧС. Вычислительная сложность алгоритма соизмерима с сложностью алгоритма построения нормы в неканонических ГЧС.

Показано, что в неканонических ГЧС, изоморфных комплексным числам и кватернионам, не существует делителей нуля.

Показан общий подход в вычислению вычетов для гиперкомплексных числовых систем. Рассмотрена процедура вычисления вычетов для неканонических ГЧС.

Показано, что процедура вычисления вычетов в общем виде неприменима к элементам в некоторых неканонических ГЧС, так как в отдельных случаях норма вычета больше нормы модуля. Рассмотрены дополнительные необходимые условия для поиска наименьшего вычета в любых неканонических ГЧС.

Показано, что вычисление вычетов возможно только тогда, если в неканонической гиперкомплексной числовой системе выполняется свойство мультипликативности нормы.

Показана реализация аналога алгоритма Евклида для неканонических ГЧС. Вычислительная сложность алгоритма Евклида зависит от сложности таблицы умножения числовой системы. Показано, что неизвестные в ходе выполнения алгоритма Евклида можно найти только в тех случаях, если ни на одном его шаге не возникают делителей нуля. Соответственно, для реализации алгоритма Евклида в неканонических ГЧС, в общем виде, необходимо выполнить проверку на появление делителей нуля. Для повышения эффективности реализации данного алгоритма, необходимо использовать числовые системы без делителей нуля.

РАЗДЕЛ 4. РЕШЕНИЕ ПРАКТИЧЕСКИХ ЗАДАЧ С ПРИМЕНЕНИЕМ НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ

В предыдущих разделах рассматривались теоретические вопросы, связанные с неканоническими гиперкомплексными числовыми системами, область практического применения которых достаточно широка. В данном разделе рассмотрено применение неканонических ГЧС к моделированию задачи разделения секрета в криптографии и синтеза структур цифровых фильтров, оптимизация их чувствительности.

4.1. Математическое моделирование задачи разделения секрета с использованием неканонических гиперкомплексных числовых систем

4.1.1. Постановка задачи разделения секрета.

Схема разделения секрета является одним из методов криптографии с открытым ключом, который сводится к задаче модулярного разделения секрета. Суть этой задачи состоит в том, как сохранить секрет, разделив его на составные части между несколькими законными пользователями. Исходная постановка задачи и ее решение были предложены в [42-44]. Поскольку разделение секрета в неканонических ГЧС базируется на исходном алгоритме для вещественных чисел, приведем его в начальном виде.

Будем говорить, что n участников (законных пользователей) A_i , $i = 1 \dots n$ осуществляют k -хранение секрета C , $1 < k \leq K_n$, если выполняются следующие три условия.

1. Каждый A_i знает некоторую информацию a_i , неизвестную любому другому участнику.
2. Секрет C может быть легко вычислен на основе любых k секретов a_i .

3. Знание любых $k-1$ частичных секретов a_i не дает возможности восстановить информацию.

Множество $\{a_1 \dots a_n\}$, удовлетворяющее этим условиям называется (n, k) пороговой схемой.

Пусть m_1, m_2, \dots, m_n – система попарно взаимно простых натуральных модулей. Предположим, что они упорядочены $m_1 < m_2 < \dots < m_n$ и выполнено условие

$$M_2 = m_1 m_2 \dots m_k > m_{n-k+1} m_{n-k+2} \dots m_n = M_1,$$

а секрет взят из промежутка (M_1, M_2) . Тогда часть секрета i -го участника a_i определяется наименьшим неотрицательным вычетом секрета x по модулю m_i . Получаем систему сравнений

$$x \equiv a_i \pmod{m_i}, i = 1 \dots n.$$

Любая подсистема из k сравнений данной системы имеет единственное решение в промежутке (M_1, M_2) . Это решение можно найти, исходя из китайской теоремы об остатках или с помощью алгоритма, основанного на кодах со смешанными основаниями [60].

Рассмотрим восстановление с помощью китайской теоремы, которая состоит в следующем [26].

Выберем совокупность попарно взаимно простых модулей m_i , $i=1..n$. Имеем a_i , $i=1..n$ – произвольные целые числа, удовлетворяющие условиям $1 \leq a_i < m_i$.

Обозначим через M произведение всех модулей m_i , $i=1..n$. Пусть далее

$$M_i = M / m_i.$$

Обозначим через N_i -число, обратное M_i по модулю m_i , $i=1..n$.

Таким образом,

$$M_i N_i \equiv 1 \pmod{m_i}.$$

Система сравнений

$$x \equiv a_i \pmod{m_i}, i = 1 \dots n$$

обладает единственным решением по модулю M , которое можно найти следующим образом:

$$x = \sum_{i=1}^n a_i M_i N_i.$$

Пусть теперь k фиксировано, $1 < k \leq n$. Обозначим через M_1 наименьшее произведение k различных модулей. Разместив модули в порядке возрастания, получим $M_1 = m_1 \times \dots \times m_k$.

Обозначим через M_2 наибольшее произведение $k-1$ модулей. Модули следует выбирать так, чтобы разность $M_1 - M_2$ была велика:

$$M_1 - M_2 \geq 3M_2.$$

Далее требуется, чтобы $M_2 < c < M_1$. В качестве секретов участников a_i возьмем наименьшие неотрицательные вычеты секрета C по модулю m_i , так что

$$a_i \equiv c \pmod{m_i}, i = 1, \dots, n.$$

Можно утверждать, что множество a_1, \dots, a_t есть (n, k) -пороговая схема для секрета C .

Докажем это. Пусть, например, известны a_1, \dots, a_k . Далее вычислим $M' = m_1 \times \dots \times m_k$, $M'_i = M' / m_i, i = 1 \dots k$ и тогда N'_i обратны к M_i по модулю m_i . Тогда можно вычислить

$$y = \sum_{i=1}^k a_i M'_i N'_i.$$

В соответствии с китайской теоремой об остатках

$$y \equiv c \pmod{M'}.$$

по имеющейся совокупности линейных сравнений может быть определена искомая величина.

Так как $M' \geq M_1 > C$, то C равно наименьшему неотрицательному вычету y по модулю M' , что дает способ вычисления, исходя из a_1, \dots, a_k .

Теперь предположим, что известны лишь a_1, \dots, a_{k-1} . Тогда

$$y \equiv c \pmod{m_1 \times \dots \times m_{k-1}}.$$

Но это оставляет много возможностей для выбора C . Таким образом, необходимо k секретов для полного восстановления исходной информации.



Рис. 4.1. Блок-схема алгоритма разделения секрета

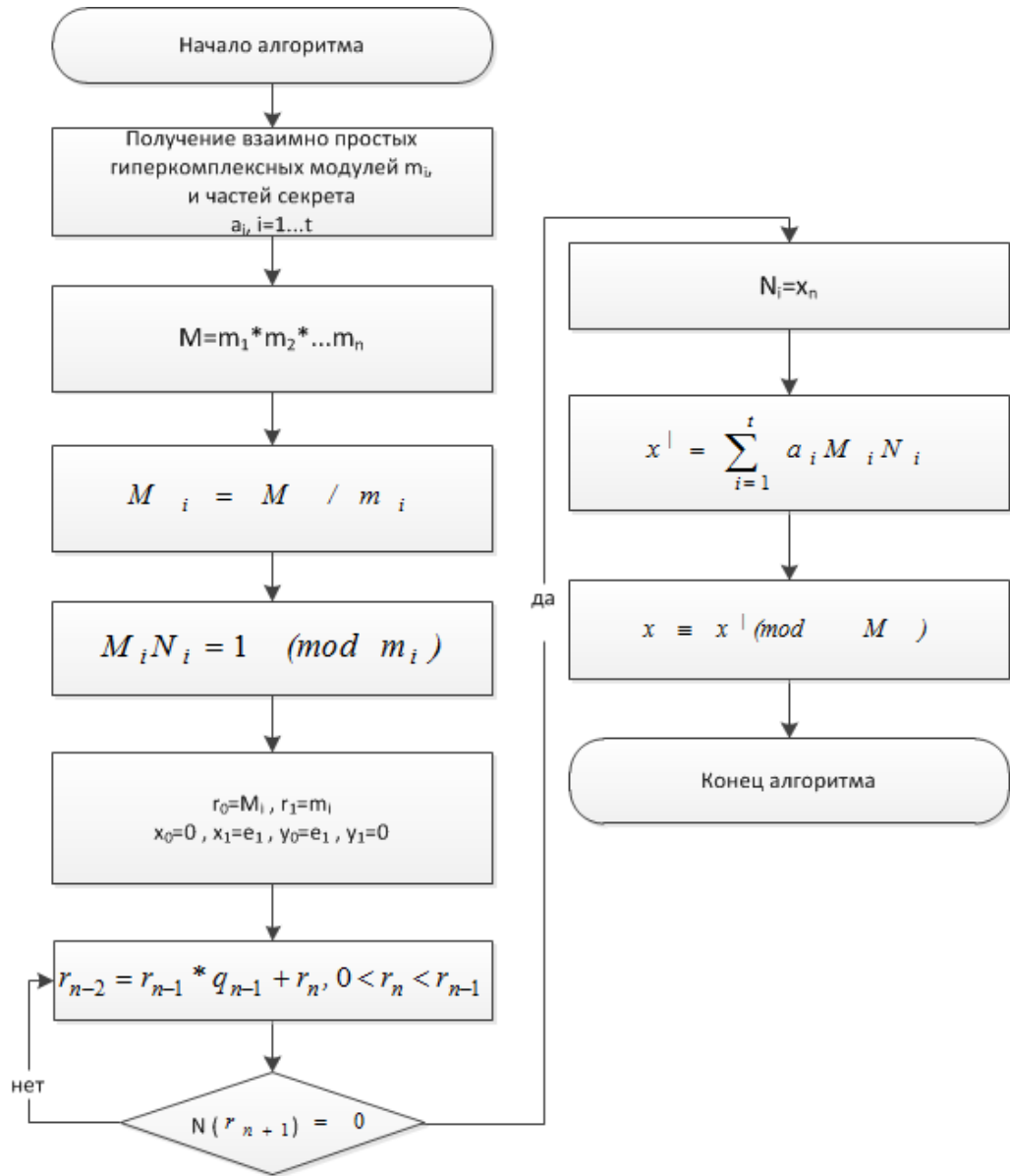


Рис. 4.2. Блок-схема алгоритма восстановления секрета

На рис 4.1 изображена блок-схема алгоритма разделения секрета, а на рис 4.2 - блок-схема алгоритма восстановления секрета в гиперкомплексных числах.

Рассмотрим процесс моделирования базовой схемы разделения секрета в неканонических гиперкомплексных числах 3-й и 4-й размерности и определим вычислительные сложности этапов этой задачи.

4.1.2. Моделирование задачи разделения секрета для неканонической гиперкомплексной числовой системы 3-й размерности.

Пусть задана неканоническая ГЧС 3-й размерности.

E_1	E_2	E_3
E_2	$-E_1 - 2E_2$	$E_1 + E_2 - E_3$
E_3	$E_1 + E_2 - E_3$	$-E_1 + 2E_3$

(4.1)

Секрет C имеет вид :

$$C = -47E_1 - 19E_2 + 53E_3.$$

Выберем три взаимнопростых модуля, т.е. такие модули, нормы которых являются взаимно простыми.

$$\begin{aligned} m_1 &= E_1 - 2E_2, \quad N(m_1) = 27, \\ m_3 &= -3E_2 + E_3, \quad N(m_3) = 64, \\ m_2 &= 5E_3, \quad N(m_2) = 125. \end{aligned} \tag{4.2}$$

Покажем область представимости секрета. В гиперкомплексных числовых системах [42-43] область представимости секрета определяется как диапазон $0 \dots N(M)$, где $N(M)$ – норма величины M , а M в свою очередь определяется соотношением:

$$M = \prod_{i=1}^n m_i.$$

При этом должно выполняться условие $0 < N(C) < N(M)$.

Соответственно, для данной системы, секрета и выбранных модулей:

$$\begin{aligned} M &= -100E_1 - 85E_2 + 75E_3, \quad N(M) = 216000, \\ N(C) &= 15625. \end{aligned}$$

Как видим, заданный секрет может быть представлен совокупностью вычетов по выбранным модулям. Вычеты в свою очередь будут равны:

$$a_1 \equiv (-47E_1 - 19E_2 + 53E_3) \pmod{E_1 - 2E_2} = -E_1 + 2E_3,$$

$$a_2 \equiv (-47E_1 - 19E_2 + 53E_3)(\text{mod } -3E_2 + E_3) = -3E_1 - 4E_2 + 4E_3, \quad (4.3)$$

$$a_3 \equiv (-47E_1 - 19E_2 + 53E_3)(\text{mod } 5E_3) = -2E_1 + E_2 + 3E_3.$$

Таким образом секрет C , представленный в неканонической гиперкомплексной числовой системе может быть представлен совокупностью вычетов (4.3) по модулям (4.2).

Восстановим секрет с помощью китайской теоремы об остатках. Вычислим систему сравнений:

$$M_1 N_1 \equiv 1(\text{mod } m_1),$$

$$M_2 N_2 \equiv 1(\text{mod } m_2),$$

...

$$M_n N_n \equiv 1(\text{mod } m_n),$$

где $M_i = M / m_i$, N_i – искомые числа, обратные M_i по модулю m_i , $i = 1 \dots n$.

Для вычисления числа N_i в области вещественных чисел можно использовать функцию Эйлера :

$$N_i = M_i^{\varphi(m_i)-1}(\text{mod } m_i),$$

которая рассмотрена только для поля вещественных чисел [1].

Для определения N_i наряду с применением функции Эйлера можно использовать и другие подходы. Это восстановление с использованием изоморфного перехода на основе фундаментальной теоремы Гаусса и ее модификациях [60], а также с применением алгоритма Евклида, который был описан ранее.

Итак, для выбранных модулей, система сравнений будет иметь вид:

$$(-20E_1 - 15E_2 + 25E_3)N_1 \equiv E_1(\text{mod } E_1 - 2E_2),$$

$$(-10E_1 - 10E_2 + 15E_3)N_2 \equiv E_1(\text{mod } -3E_2 + E_3), \quad (4.4)$$

$$(-8E_1 - 17E_2 + 3E_3)N_3 \equiv E_1(\text{mod } 5E_3).$$

Выполняем последовательно шаги алгоритма Евклида для каждого из сравнений:

$$1) (-20E_1 - 15E_2 + 25E_3)N_1 \equiv E_1 \pmod{E_1 - 2E_2},$$

Инициализируем начальные значения:

$$r_0 = -20E_1 - 15E_2 + 25E_3, \quad x_0 = E_1, \quad y_0 = 0,$$

$$r_1 = E_1 - 2E_2, \quad x_1 = 0, \quad y_1 = E_1.$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{-20E_1 - 15E_2 + 25E_3}{E_1 - 2E_2} = \frac{-60E_1 - 15E_2 + 225E_3}{27},$$

$$-60 \pmod{27} \equiv -6, \quad -15 \pmod{27} \equiv 12, \quad 225 \pmod{27} \equiv 9,$$

$$\Rightarrow r_2 = \frac{(-6E_1 + 12E_2 + 9E_3)(E_1 - 2E_2)}{27} = 2E_2 + E_3,$$

$$q_1 = \frac{-20E_1 - 17E_2 + 24E_3}{E_1 - 2E_2} = -2E_1 - E_2 + 8E_3,$$

$$x_2 = x_0 - q_1x_1 = E_1 - (-2E_1 - E_2 + 8E_3) \cdot 0 = E_1,$$

$$N(r_2) = -1,$$

$$N_1 = X = x_2 / (2E_2 + E_3) = -2E_1 - 2E_2 - E_3.$$

$$2) (-10E_1 - 10E_2 + 15E_3)N_2 \equiv E_1 \pmod{-3E_2 + E_3},$$

Инициализируем начальные значения:

$$r_0 = -10E_1 - 10E_2 + 15E_3, \quad x_0 = E_1, \quad y_0 = 0,$$

$$r_1 = -3E_2 + E_3, \quad x_1 = 0, \quad y_1 = E_1.$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{-10E_1 - 10E_2 + 15E_3}{-3E_2 + E_3} = \frac{80E_1 + 20E_2 + 180E_3}{64},$$

$$80 \pmod{64} \equiv 16, \quad 20 \pmod{64} \equiv 20, \quad 180 \pmod{64} \equiv 52,$$

$$\Rightarrow r_2 = \frac{(16E_1 + 20E_2 + 52E_3)(-3E_2 + E_3)}{64} = -2E_1 - E_2 + 4E_3,$$

$$q_1 = \frac{-8E_1 - 9E_2 + 11E_3}{-3E_2 + E_3} = E_1 + 2E_3,$$

$$x_2 = x_0 - q_1x_1 = E_1 - (E_1 + 2E_3) \cdot 0 = E_1,$$

$$\frac{r_1}{r_2} = \frac{-3E_2 + E_3}{-2E_1 - E_2 + 4E_3} = \frac{60E_1 - 15E_2 - 39E_3}{27}$$

$$60 \bmod(27) \equiv 6, \quad -15 \bmod(27) \equiv 12, \quad -39 \bmod(27) \equiv -12,$$

$$\Rightarrow r_3 = \frac{(6E_1 + 12E_2 - 12E_3)(-2E_1 - E_2 + 4E_3)}{27} = 4E_1 + 2E_2 - 4E_3,$$

$$q_2 = \frac{-4E_1 - 5E_2 + 5E_3}{-2E_1 - E_2 + 4E_3} = 2E_1 - E_2 - E_3,$$

$$x_3 = x_1 - q_2 x_2 = 0 - (2E_1 - E_2 - E_3) * E_1 = -2E_1 + E_2 + E_3,$$

$$\frac{r_2}{r_3} = \frac{-2E_1 - E_2 + 4E_3}{4E_1 + 2E_2 - 4E_3} = \frac{28E_1 + 8E_2 - 8E_3}{-8},$$

$$28 \bmod(-8) \equiv 4, \quad 8 \bmod(-8) \equiv 0, \quad -8 \bmod(-8) \equiv 0,$$

$$\Rightarrow r_4 = \frac{(4E_1)(4E_1 + 2E_2 - 4E_3)}{-8} = -2E_1 - E_2 + 2E_3,$$

$$q_3 = \frac{-6E_1 - E_2 + 4E_3}{4E_1 + 2E_2 - 4E_3} = -3E_1 - E_2 + E_3,$$

$$x_4 = x_2 - q_3 x_3 = -2E_1 - E_2 + 4E_3 - \\ -(-3E_1 - E_2 + E_3)(-2E_1 + E_2 + E_3) = -8E_1 - 2E_2 + 5E_3,$$

$$N(r_4) = 1,$$

$$N_2 = X = x_4 / (-2E_1 - E_2 + 2E_3) = -8E_1 - 2E_2 + 5E_3.$$

$$3) (-8E_1 - 17E_2 + 3E_3)N_3 \equiv E_1 \pmod{5E_3},$$

Инициализируем начальные значения:

$$r_0 = -8E_1 - 17E_2 + 3E_3, \quad x_0 = E_1, \quad y_0 = 0,$$

$$r_1 = 5E_3, \quad x_1 = 0, \quad y_1 = E_1.$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{-8E_1 - 17E_2 + 3E_3}{5E_3} = \frac{100E_1 - 425E_2 - 225E_3}{125}$$

$$100 \bmod(125) \equiv 25, \quad -425 \bmod(125) \equiv 75, \quad -225 \bmod(125) \equiv 25,$$

$$\Rightarrow r_2 = \frac{(25E_1 + 75E_2 + 25E_3)(5E_3)}{125} = 2E_1 + 3E_2 + 3E_3,$$

$$q_1 = \frac{-10E_1 - 20E_2}{5E_3} = -4E_2 - 2E_3,$$

$$x_2 = x_0 - q_1 x_1 = E_1 - (-4E_2 - 2E_3) \cdot 0 = E_1,$$

$$\frac{r_1}{r_2} = \frac{5E_3}{2E_1 + 3E_2 + 3E_3} = \frac{-30E_2 - 10E_3}{8}$$

$$-30 \bmod(8) \equiv 2, \quad -10 \bmod(8) \equiv -2,$$

$$\Rightarrow r_2 = \frac{(2E_2 - 2E_3)(2E_1 + 3E_2 + 3E_3)}{8} = -E_2 - 2E_3,$$

$$N(r_2) = -1,$$

$$x_2 = x_0 - qx_1 = E_1 - (-E_2 - 2E_3) \cdot 0 = E_1,$$

$$N_3 = X = x_2 / (-E_2 - 2E_3) = 3E_1 - 7E_2 - 7E_3.$$

$$Y = a_1M_1N_1 + a_2M_2N_2 + a_3M_3N_3 = -387E_1 - 29E_2 + 263E_3.$$

Тогда секрет C будет равен:

$$C \equiv Y \pmod{M} = (-387E_1 - 29E_2 + 263E_3) \pmod{-100E_1 - 85E_2 + 75E_3} = -47E_1 - 19E_2 + 53E_3$$

4.1.3. Моделирование задачи разделения секрета для неканонической гиперкомплексной числовой системы 4-й размерности.

Рассмотрим моделирование задачи разделения секрета в неканонической гиперкомплексной числовой системы 4-й размерности, изоморфной кватернионам.

Пусть задана неканоническая ГЧС 4-й размерности.

E_1	E_2	E_3	E_4	(4.5)
E_2	$-2E_2 + 2E_3 - 4E_4$	$-4E_1 - 2E_2 - 2E_3$	$-E_3$	
E_3	$-4E_1 - 2E_2 - 2E_3$	$2E_2 - 2E_3 + 4E_4$	E_2	
E_4	$-E_3$	E_2	$-E_1$	

Секрет C имеет вид :

$$C = 3E_1 - E_2 + 4E_3 - 8E_4.$$

Выберем три взаимнопростых модуля, т.е. такие модули, нормы которых являются взаимно простыми.

$$\begin{aligned}
m_1 &= E_1 + E_3 - 2E_4, & N(m_1) &= 4, \\
m_2 &= E_1 + 2E_3 + 2E_4, & N(m_2) &= 481, \\
m_3 &= 2E_1 + E_2 - E_3 + 3E_4, & N(m_3) &= 17.
\end{aligned} \tag{4.6}$$

Покажем область представимости секрета. Соответственно, для данной системы, секрета и выбранных модулей:

$$\begin{aligned}
M &= \prod_{i=1}^3 m_i = 3E_1 - E_2 + 4E_3 - 8E_4, & N(M) &= 32708, \\
N(C) &= 1525.
\end{aligned}$$

Как видим, заданный секрет может быть представлен совокупностью вычетов по выбранным модулям. Вычеты в свою очередь будут равны:

$$\begin{aligned}
a_1 &\equiv (3E_1 - E_2 + 4E_3 - 8E_4) \pmod{E_1 + E_3 - E_4} = E_1 + E_2 + 2E_4, \\
a_2 &\equiv (3E_1 - E_2 + 4E_3 - 8E_4) \pmod{E_1 + 2E_3 + 2E_4} = -3E_1 + 2E_2 - E_3 + 4E_4, \\
a_3 &\equiv (3E_1 - E_2 + 4E_3 - 8E_4) \pmod{2E_1 - E_2 - E_3 + 3E_4} = E_1 + E_2 + E_3 - 3E_4.
\end{aligned} \tag{4.7}$$

Таким образом секрет C , представленный в неканонической гиперкомплексной числовой системе может быть представлен совокупностью вычетов (4.7) по модулям (4.6).

Восстановим секрет с помощью китайской теоремы об остатках. Для выбранных модулей, система сравнений будет иметь вид:

$$\begin{aligned}
(-12E_1 - 3E_2 + E_3 - E_4)N_1 &\equiv E_1 \pmod{E_1 + E_3 - E_4}, \\
(E_1 + E_2 + 2E_3 - 3E_4)N_2 &\equiv E_1 \pmod{E_1 + 2E_3 + 2E_4}, \\
(3E_1 + 4E_2 - E_3 + 9E_4)N_3 &\equiv E_1 \pmod{2E_1 - E_2 - E_3 + 3E_4}.
\end{aligned} \tag{4.8}$$

Выполняем последовательно шаги алгоритма Евклида для каждого из сравнений:

$$1) \quad (-12E_1 - 3E_2 + E_3 - E_4)N_1 \equiv E_1 \pmod{E_1 + E_3 - E_4},$$

Инициализируем начальные значения:

$$\begin{aligned}
r_0 &= -12E_1 - 3E_2 + E_3 - E_4, & x_0 &= E_1, & y_0 &= 0, \\
r_1 &= E_1 + E_3 - E_4, & x_1 &= 0, & y_1 &= E_1.
\end{aligned}$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{-12E_1 - 3E_2 + E_3 - E_4}{E_1 + E_3 - E_4} = \frac{30E_1 + 20E_2 + 6E_3 + 2E_4}{4}$$

$$30 \bmod(4) \equiv 2, \quad 20 \bmod(4) \equiv 0,$$

$$6 \bmod(4) \equiv 2, \quad 2 \bmod(4) \equiv 2.$$

$$\Rightarrow r_2 = \frac{(2E_1 + 2E_3 + 2E_4)(E_1 + E_3 - E_4)}{4} = E_1 + E_2 + 2E_4,$$

$$q_1 = \frac{-13E_1 - 4E_2 + E_3 - E_4}{E_1 + E_3 - E_4} = 7E_1 + 5E_2 + E_3,$$

$$x_2 = x_0 - q_1 x_1 = E_1 - (7E_1 + 5E_2 + E_3) \cdot 0 = E_1,$$

$$\frac{r_1}{r_2} = \frac{E_1 + E_3 - E_4}{E_1 + E_2 + 2E_4} = \frac{-E_1 - E_2 + 2E_3 - 7E_4}{5},$$

$$-1 \bmod(5) \equiv -1, \quad -1 \bmod(5) \equiv -1,$$

$$2 \bmod(5) \equiv 2, \quad -7 \bmod(5) \equiv -2.$$

$$\Rightarrow r_3 = \frac{(-E_1 - E_2 + 2E_3 - 2E_4)(E_1 + E_2 + 2E_4)}{5} = -E_1,$$

$$q_2 = \frac{2E_1 + E_3 - E_4}{E_1 + E_2 + 2E_4} = -E_4,$$

$$x_3 = x_1 - q_2 x_2 = 0 - (-E_4) \cdot E_1 = E_4,$$

$$N(r_3) = 1,$$

$$N_1 = X = x_3 / (-E_1) = -E_4.$$

$$2) (E_1 + E_2 + 2E_3 - 3E_4)N_2 \equiv E_1 \pmod{E_1 + 2E_3 + 2E_4},$$

Инициализируем начальные значения:

$$r_0 = E_1 + E_2 + 2E_3 - 3E_4, \quad x_0 = E_1, \quad y_0 = 0,$$

$$r_1 = E_1 + 2E_3 + 2E_4, \quad x_1 = 0, \quad y_1 = E_1.$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{E_1 + E_2 + 2E_3 - 3E_4}{E_1 + 2E_3 + 2E_4} = \frac{-329E_1 - 197E_2 - 146E_3 + 383E_4}{481}$$

$$-329 \bmod(481) \equiv 152, \quad -197 \bmod(481) \equiv 284,$$

$$-146 \bmod(481) \equiv -146, \quad 383 \bmod(481) \equiv 383,$$

$$\begin{aligned} \Rightarrow r_2 &= \frac{(152E_1 + 284E_2 - 146E_3 + 383E_4)(E_1 + 2E_3 + 2E_4)}{481} = \\ &= -6E_1 - 2E_2 - 2E_3 - E_4 \end{aligned}$$

$$q_1 = \frac{7E_1 + 3E_2 + 4E_3 - 2E_4}{E_1 + 2E_3 + 2E_4} = -E_1 - E_2,$$

$$x_2 = x_0 - q_1 x_1 = E_1 - (-E_1 - E_2) \cdot 0 = E_1,$$

$$\frac{r_1}{r_2} = \frac{E_1 + 2E_3 + 2E_4}{-6E_1 - 2E_2 - 2E_3 - E_4} = \frac{-152E_1 + 132E_2 + 250E_3 + 409E_4}{377},$$

$$-152 \bmod(377) \equiv 225, \quad 132 \bmod(377) \equiv 132,$$

$$-250 \bmod(377) \equiv 127, \quad 409 \bmod(377) \equiv 32,$$

$$\begin{aligned} \Rightarrow r_3 &= \frac{(225E_1 + 132E_2 - 250E_3 + 32E_4)(-6E_1 - 2E_2 - 2E_3 - E_4)}{377} = \\ &= 2E_1 - E_2 - E_4 \end{aligned}$$

$$q_2 = \frac{-E_1 + E_2 + 2E_3 + 3E_4}{-6E_1 - 2E_2 - 2E_3 - E_4} = -E_1 - E_3 + E_4,$$

$$x_3 = x_1 - q_2 x_2 = 0 - (-E_1 - E_3 + E_4)E_1 = E_1 + E_3 - E_4,$$

$$\frac{r_2}{r_3} = \frac{-6E_1 - 2E_2 - 2E_3 - E_4}{2E_1 - E_2 - E_4} = \frac{-139E_1 - 62E_2 - 61E_3 + 12E_4}{85},$$

$$-139 \bmod(85) \equiv 31, \quad -62 \bmod(85) \equiv 23,$$

$$-61 \bmod(85) \equiv 24, \quad 12 \bmod(85) \equiv 12,$$

$$\begin{aligned} \Rightarrow r_4 &= \frac{(31E_1 + 23E_2 + 24E_3 + 12E_4)(4E_1 + 2E_2 - 4E_3)}{85} = \\ &= 2E_1 + E_2 + E_3 + E_4 \end{aligned}$$

$$q_3 = \frac{-8E_1 - 3E_2 - 3E_3 - 2E_4}{2E_1 - E_2 - E_4} = -2E_1 - E_2 - E_3,$$

$$x_4 = x_2 - q_3 x_3 = E_1 - (-2E_1 - E_2 - E_3)(E_1 + E_3 - E_4) = -E_1 + 2E_4,$$

$$\frac{r_3}{r_4} = \frac{2E_1 - E_2 - E_4}{2E_1 + E_2 + E_3 + E_4} = \frac{-6E_1 - 3E_2 - 3E_3 + 3E_4}{9},$$

$$-6 \bmod(9) \equiv 3, \quad -3 \bmod(9) \equiv -3,$$

$$-3 \bmod(9) \equiv -3, \quad 3 \bmod(9) \equiv 3,$$

$$\Rightarrow r_5 = \frac{(3E_1 - 3E_2 - 3E_3 + 3E_4)(2E_1 + E_2 + E_3 + E_4)}{85} = -2E_1 - E_3 + E_4,$$

$$q_4 = \frac{4E_1 - E_2 + E_3}{2E_1 + E_2 + E_3 + E_4} = -2E_1 - E_2 - E_3,$$

$$x_5 = x_3 - q_4 x_4 = E_1 + E_3 - E_4 - (-2E_1 - E_2 - E_3)(-E_1 + 2E_4) = -E_1 + E_2 - 2E_3 + 3E_4,$$

$$\frac{r_4}{r_5} = \frac{2E_1 + E_2 + E_3 + E_4}{-2E_1 - E_3 + E_4} = \frac{-7E_1 - 2E_2 - E_3 - 4E_4}{5},$$

$$-7 \bmod(5) \equiv -2, \quad -2 \bmod(5) \equiv -2,$$

$$-1 \bmod(5) \equiv -1, \quad -4 \bmod(5) \equiv 1,$$

$$\Rightarrow r_6 = \frac{(-2E_1 + E_2 - 2E_3 + E_4)(-2E_1 - E_3 + E_4)}{5} = -E_1,$$

$$q_5 = \frac{3E_1 + E_2 + E_3 + E_4}{-2E_1 - E_3 + E_4} = -E_1 - E_4,$$

$$x_6 = x_4 - q_5 x_5 = -E_1 + 2E_4 - (-E_1 - E_4)(-E_1 + E_2 - 2E_3 + 3E_4) = -5E_1 - E_2 - 3E_3 + 4E_4,$$

$$N(r_6) = 1,$$

$$N_2 = X = x_6 / (-E_1) = 5E_1 + E_2 + 3E_3 - 4E_4.$$

$$3) (3E_1 + 4E_2 - E_3 + 9E_4)N_3 \equiv E_1 \pmod{2E_1 + E_2 - E_3 + 3E_4},$$

Инициализируем начальные значения:

$$r_0 = 3E_1 + 4E_2 - E_3 + 9E_4, \quad x_0 = E_1, \quad y_0 = 0,$$

$$r_1 = 2E_1 + E_2 - E_3 + 3E_4, \quad x_1 = 0, \quad y_1 = E_1.$$

Находим промежуточные значения:

$$\frac{r_0}{r_1} = \frac{3E_1 + 4E_2 - E_3 + 9E_4}{2E_1 + E_2 - E_3 + 3E_4} = \frac{113E_1 - 3E_2 + 46E_3 - 7E_4}{17}$$

$$113 \bmod(20) \equiv 11, \quad -3 \bmod(20) \equiv -3,$$

$$46 \bmod(20) \equiv 6, \quad -7 \bmod(20) \equiv -7.$$

$$\Rightarrow r_2 = \frac{(11E_1 - 3E_2 + 6E_3 - 7E_4)(2E_1 + E_2 - E_3 + 3E_4)}{17} = -E_1 + E_2 - E_3,$$

$$q_1 = \frac{4E_1 + 3E_2 + 9E_4}{2E_1 + E_2 - E_3 + 3E_4} = 6E_1 + 2E_3,$$

$$x_2 = x_0 - q_1 x_1 = E_1 - (-4E_2 - 2E_3) \cdot 0 = E_1,$$

$$\frac{r_1}{r_2} = \frac{2E_1 + E_2 - E_3 + 3E_4}{-E_1 + E_3 - E_4} = \frac{-14E_1 - 12E_2 + 6E_3 - 22E_4}{20},$$

$$-14 \bmod(20) \equiv 6, \quad -12 \bmod(20) \equiv 8,$$

$$6 \bmod(20) \equiv 6, \quad -22 \bmod(20) \equiv -2,$$

$$\Rightarrow r_3 = \frac{(6E_1 + 8E_2 + 6E_3 - 2E_4)(-E_1 + E_3 - E_4)}{20} = -2E_1 - E_2 - E_3 + E_4,$$

$$q_2 = \frac{4E_1 + 2E_2 + 2E_4}{-E_1 + E_3 - E_4} = -E_1 - E_2 - E_4,$$

$$x_3 = x_1 - q_2 x_2 = 0 - (-E_1 - E_2 - E_4)E_1 = E_1 + E_2 + E_4,$$

$$\frac{r_2}{r_3} = \frac{-E_1 + E_3 - E_4}{-2E_1 - E_2 - E_3 + E_4} = \frac{-15E_1 - 3E_2 - 6E_3 + 3E_4}{9},$$

$$-15 \bmod(9) \equiv 3, \quad -3 \bmod(9) \equiv -3,$$

$$-6 \bmod(9) \equiv 3, \quad 3 \bmod(9) \equiv 3,$$

$$\Rightarrow r_4 = \frac{(3E_1 - 3E_2 + 3E_3 + 3E_4)(-2E_1 - E_2 - E_3 + E_4)}{9} = -E_1 - E_2 + E_3 - 3E_4,$$

$$q_3 = -2E_1 - E_3,$$

$$x_4 = x_2 - q_3 x_3 = E_1 - (-2E_1 - E_3)(E_1 + E_2 + E_4) = -E_1 + E_2 - E_3 + 2E_4,$$

$$\frac{r_3}{r_4} = \frac{-2E_1 - E_2 - E_3 + E_4}{-E_1 - E_2 + E_3 - 3E_4} = \frac{6E_1 - 2E_2 + 6E_3 - 2E_4}{20},$$

$$6 \bmod(20) \equiv 6, \quad -2 \bmod(20) \equiv -2,$$

$$6 \bmod(20) \equiv 6, \quad -2 \bmod(20) \equiv -2,$$

$$\Rightarrow r_5 = \frac{(6E_1 - 2E_2 + 6E_3 - 2E_4)(-E_1 - E_2 + E_3 - 3E_4)}{20} = E_1,$$

$$q_4 = -E_4, \quad N(r_5) = 1,$$

$$x_5 = x_3 - q_4 x_4 = E_1 + E_2 + E_4 - (-E_4)(-E_1 + E_2 - E_3 + 2E_4) = -E_1 - E_3,$$

$$N_3 = X = x_5 / (E_1) = -E_1 - E_3.$$

$$Y = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = -57E_1 - 33E_2 - 18E_3 + 60E_4.$$

Тогда секрет C будет равен:

$$C \equiv Y(\bmod M) = (-57E_1 - 33E_2 - 18E_3 + 60E_4)(\bmod -E_1 + 3E_2 - 10E_3 + 15E_4) = 3E_1 - E_2 + 4E_3 - 8E_4.$$

Немотря на то, что сложность вычислений повышается за счет сложности таблицы умножения числовой системы, но при этом повышается стойкость схемы разделения секрета, что будет исследовано далее.

Рассмотрим вычислительную сложность задачи разделения секрета для канонической ГЧС размерности n и $n+1$, а также неканонической ГЧС размерности n с одной составной и $(n-1)^2$ составными ячейками. При этом предполагается, что у данных систем единичный элемент в базисе (Таблица 1). Число m в оценке восстановления секрета предполагает длину ключа [39].

Таблица 4.1 Вычислительная сложность задачи разделения секрета в ГЧС

Тип ГЧС	Разделение секрета (вычисление вычета)	Восстановление секрета с помощью алгоритма Евклида
Каноническая ГЧС размерности n	$O(n^2 + n \cdot n!)$	$O(n^2 + n \cdot n! + \text{Ln}(m(n^2 + n \cdot n!)))$
Каноническая ГЧС размерности $n+1$	$O(n^2 + (n+1)(n+1)!)$	$O(n^2 + (n+1)(n+1)! + \text{Ln}(m(n^2 + (n+1) \cdot (n+1)!)))$
Неканоническая ГЧС размерности n с одной составной ячейкой	$O(n^2 + n \cdot n!)$	$O(n^2 + n \cdot n! + \text{Ln}(m(n^2 + n \cdot n!)))$
Неканоническая ГЧС размерности n с $(n-1)^2$ составных ячеек	$O(n^3 + n \cdot n!)$	$O(n^3 + n \cdot n! + \text{Ln}(m(n^3 + n \cdot n!)))$

Очевидно, что вычислительная процедура разделения секрета в неканонической ГЧС размерности n с $(n-1)^2$ составной ячейкой, сложнее, чем аналогичная процедура в канонической ГЧС размерности $n+1$. То же самое можно сказать и про процедуру восстановления секрета.

Для повышения криптостойкости задачи разделения секрета при работе с каноническими гиперкомплексными числами необходимо было повышать размерность гиперкомплексной числовой системы. Учитывая вышесказанное, можно сделать вывод, что для повышения стойкости задачи разделения секрета целесообразно представлять данные в неканонических гиперкомплексных числовых системах той же размерности, с более сложной структурой таблицы умножения.

Сложность взлома схемы разделения секрета злоумышленником в канонических ГЧС была рассмотрена в [44]. Покажем вычислительные сложности подбора гиперкомплексной числовой системы злоумышленником, - а фактически, процедуры перебора гиперкомплексных числовых систем с единицей в базисе в таблице 4.2.

Таблица 4.2 Вычислительная сложность подбора числовых систем злоумышленником.

Тип ГЧС	Оценка сложности подбора ГЧС
Каноническая ГЧС размерности n	$O(2n^3 - 3n^2 + 1)$
Каноническая ГЧС размерности $n+1$	$O(2n^3 + 3n^2)$
Неканоническая ГЧС размерности n с одной составной ячейкой	$O(2n^3 - 3n^2 + 3n)$
Неканоническая ГЧС размерности n с $(n-1)^2$ составных ячеек	$O(3n^3 - 6n^2 + 3n)$
Неканоническая ГЧС размерности n с $(n-1)^2$ составных ячеек с целыми коэффициентами при базисных элементах из диапазона $\{-t..t\}$	$O((2t+1)(n^3 - 2n^2 + n))$

На рис. 4.3 и 4.4 показаны зависимости, представленные в таблице 4.2. Рис. 4.3 показывает, что для обеспечения такой же криптостойкости, то есть необходимого количества операций для подбора числовой системы, как и для

канонической ГЧС размерности 4, достаточно неканонической ГЧС размерности 3 с целыми коэффициентами при базисных элементах из диапазона $\{-2..2\}$. На рис. 4.4 показано, что для канонической ГЧС размерности 6 и неканонической ГЧС размерности 4 с целыми коэффициентами из диапазона $\{-4..4\}$, обеспечивается примерно одинаковая криптостойкость.

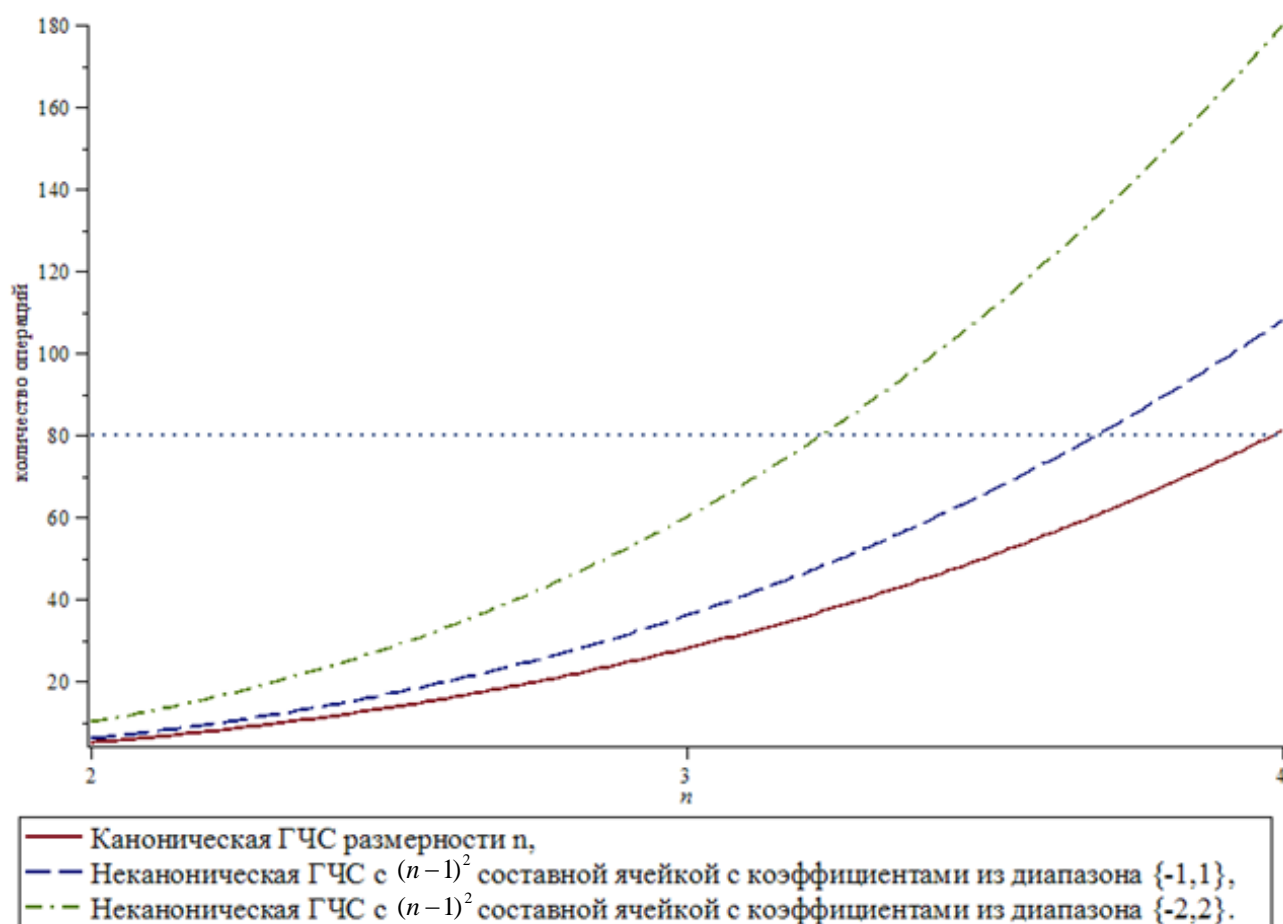


Рис. 4.3. Сравнительные графики сложностей алгоритма подбора ГЧС злоумышленником для разных видов ГЧС.

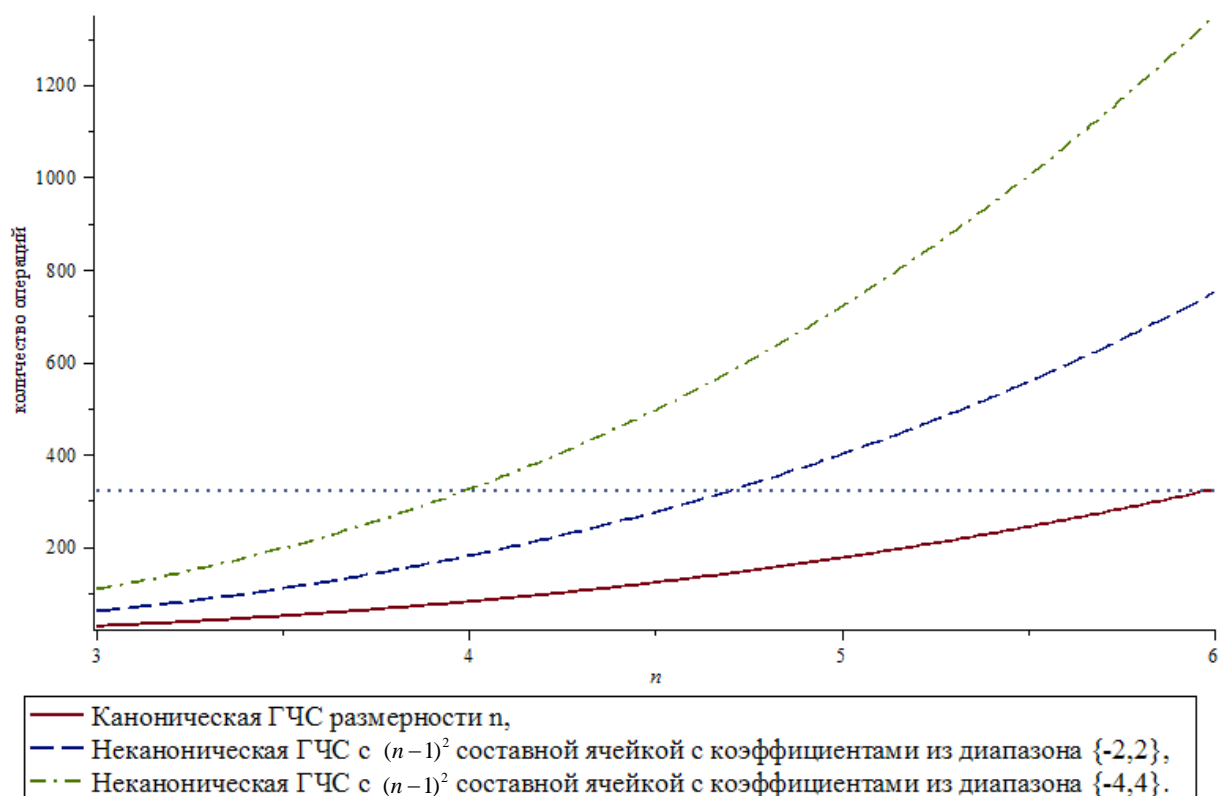


Рис. 4.4. Сравнительные графики сложностей алгоритма подбора ГЧС злоумышленником для разных видов ГЧС.

Можно утверждать, что сложность подборов канонической гиперкомплексной числовой системы размерности $n+1$ и неканонической гиперкомплексной числовой системы размерности n практически одинаковы. Но, если учитывать, что коэффициентами при структурных элементах могут быть целые числа из диапазона $\{-t..t\}$, вычислительная сложность значительно возрастает, что подтверждает вывод о целесообразности и эффективности использования неканонических гиперкомплексных чисел в задаче разделения секрета.

В таблице 4.3 представлены данные по количеству умножений для этапов задачи разделения секрета, полученные эмпирическим путем. В таблице 4.4 показано изменение количества умножений для таких этапов для сравнимых по криптостойкости канонической и неканонической гиперкомплексных числовых систем. Как видно из таблицы 4.4 использование неканонических ГЧС для

повышения стойкости задачи разделения секрета целесообразно при $t \geq 3$ и $n \geq 3$.

Изменения количества вычислений определялись по формуле:

$$\frac{V_2 - V_1}{V_1} \cdot 100\%,$$

где V_1 - среднее количество операций для канонической ГЧС, а V_2 - среднее количество операций для неканонической ГЧС заданного вида.

Таблица 4.3 Среднее количество умножений для этапов работы модели разделения секрета в зависимости от вида гиперкомплексной числовой системы.

Вид ГЧС	Представление данных в ГЧС (изоморфные переходы)	Вычисление вычета в ГЧС	Восстановление секрета с помощью алгоритма Евклида
Каноническая ГЧС размерности 4	160	160	364
Неканоническая ГЧС размерности 3 с $(n-1)^2$ составных ячеек в таблице умножения с целыми коэффициентами из диапазона $\{-2..2\}$	198	470	651
Каноническая ГЧС размерности 6	4392	4464	4733
Неканоническая ГЧС размерности 4 с $(n-1)^2$ составных ячеек в таблице умножения с целыми коэффициентами из диапазона $\{-4..4\}$	1568	3292	2855

Таблица 4.4 Изменение количества операций для сравнимых по криптостойкости канонической и неканонической ГЧС.

Сравнимые ГЧС по криптостойкости в задаче разделения секрета	Представление данных в ГЧС с помощью изоморфных переходов	Вычисление вычета в ГЧС	Восстановление секрета с помощью алгоритма Евклида
Каноническая ГЧС размерности 4 и неканоническая ГЧС размерности 3 с $(n-1)^2$ составных ячеек в таблице умножения с целыми коэффициентами из диапазона $\{-2..2\}$	+23%	+194%	+79%
Каноническая ГЧС размерности 6 и неканоническая ГЧС размерности 4 с $(n-1)^2$ составных ячеек в таблице умножения с целыми коэффициентами из диапазона $\{-4..4\}$	-64%	-24%	-36%

Как видно из таблицы 4.4, использование неканонической ГЧС размерности 3 для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 4, не дает нужного эффекта по минимизации вычислений, так как количество умножений увеличивается в среднем на 92%. Но при использовании неканонической ГЧС размерности 4 с 9 составными ячейками в таблице умножения с коэффициентами из диапазона $\{-4..4\}$, для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 6, количество требуемых вычислений уменьшается в среднем на 44%.

4.2. Синтез структур цифровых фильтров с оптимизированной чувствительностью в неканонических гиперкомплексных числовых системах

4.2.1. Эквивалентирование цифрового фильтра с вещественными коэффициентами и фильтра с гиперкомплексными коэффициентами.

Построение цифровых фильтров с использованием гиперкомплексного представления данных было рассмотрено в работах [35-37, 65-70, 110]. Рассмотрим теоретические основы этого метода.

Передаточная функция рекурсивного цифрового фильтра l -го порядка представляет собой отношение двух полиномов степени l от оператора временного сдвига z :

$$H(z) = \frac{X(z)}{Y(z)}. \quad (4.11)$$

Для традиционных цифровых фильтров у полиномов $X(z)$ и $Y(z)$ вещественные коэффициенты. Будем предполагать, что эти коэффициенты – гиперкомплексные числа, принадлежащие ГЧС Γ размерности n с единичным элементом E . Тогда $H(z)$, $X(z)$ и $Y(z)$ – будут гиперкомплексными функциями и иметь вид:

$$X(z) = \sum_{i=0}^l x_i z^{-i}, \quad Y(z) = \sum_{i=0}^l y_i z^{-i}, \quad x_0 = 1.$$

Преобразуем передаточную функцию (4.11) с гиперкомплексными коэффициентами $q_i \in \Gamma$ в форму гиперкомплексной функции, то есть функции вида:

$$f(X) = \sum_{i=1}^m f_i(x_1, \dots, x_m) \cdot e_i,$$

где: $X = \sum_{i=1}^m x_i e_i \in \Gamma$;

e_i , $i = 1, \dots, m$ – базисные элементы системы Γ .

Для такого преобразования нужно числитель и знаменатель (4.11) умножить на такой гиперкомплексный множитель, чтобы в знаменателе осталось гиперкомплексное число вида $N \cdot E$, где N - вещественное число.

Как было показано в разделе 3, таким множителем является $\overline{Y(z)}$, то есть сопряженное числу $Y(z)$, а произведение $Y(z) \cdot \overline{Y(z)}$ - норма гиперкомплексного числа $Y(z)$ - $N(Y(z))$. Нормой гиперкомплексного числа является форма m -й степени от компонентов этого числа. Поскольку $Y(z)$ - полином степени l , то норма $N(Y(z))$ будет формой степени $l \cdot m$ относительно оператора z .

Соответственно и сопряженное число $\overline{Y(z)}$ будет формой степени $l(m-1)$, а произведение $X(z) \cdot \overline{Y(z)}$ будет формой степени m относительно элементов гиперкомплексного числа, а относительно оператора z - степени $m \cdot l$.

Таким образом, передаточная функция (4.11), но с гиперкомплексными коэффициентами, преобразовывается в функцию, которую, в свою очередь, можно представить в виде гиперкомплексной функции:

$$H(z) = \frac{X(z) \cdot \overline{Y(z)}}{N(Y(z))} = \sum_{i=1}^m \frac{f_i(z)}{N(Y(z))} \cdot e_i, \quad (4.12)$$

При этом, коэффициенты при операторе z в выражениях $\frac{f_i(z)}{N(X(z))}$, ($i = 1, \dots, n$), принадлежат области вещественных чисел. А сами выражения

$\frac{f_i(z)}{N(X(z))}$, будут компонентами гиперкомплексного числа с базисом e_1, e_2, \dots, e_n .

Кроме того, полином $f_i(z)$, также, как и $N(X(z))$, имеет степень $n \cdot l$ относительно оператора z .

Следуя методике, описанной выше, цифровой фильтр n -го порядка с вещественными коэффициентами можно эквивалентировать цифровым фильтром первого порядка с гиперкомплексными коэффициентами A, B, C , принадлежащим ГЧС размерности n , с передаточной функцией:

$$H_{\Gamma} = \frac{A + Bz^{-1}}{1 + Cz^{-1}} = \frac{(A + Bz^{-1}) \cdot \overline{(1 + Cz^{-1})}}{N(1 + Cz^{-1})}. \quad (4.13)$$

4.2.2. Синтез неканонических ГЧС, удовлетворяющих условиям построения цифрового фильтра.

Для построения цифрового фильтра с гиперкомплексными коэффициентами в неканонической ГЧС, необходимо получить множество систем, удовлетворяющих условиям построения такого фильтра.

Необходимым условием, накладываемым на неканоническую ГЧС, пригодную для построения цифрового фильтра, является присутствие всех гиперкомплексных коэффициентов в (4.13).

Возьмем за основу алгоритм перечисления неканонических ГЧС размерности 3, изоморфных системе прямой суммы вещественных чисел, описанным в разделе 2.2. В результате получим список линейно независимых систем, с единицей в базисе, с таблицей умножения такого вида:

	e_1	e_2	e_3
$\Gamma_{40}(e,3)$	e_2	$\gamma_{1_{22}}e_1 + \gamma_{2_{22}}e_2 + \gamma_{3_{22}}e_3$	$\gamma_{1_{23}}e_1 + \gamma_{2_{23}}e_2 + \gamma_{3_{23}}e_3$
	e_3	$\gamma_{1_{23}}e_1 + \gamma_{2_{23}}e_2 + \gamma_{3_{23}}e_3$	$\gamma_{1_{33}}e_1 + \gamma_{2_{33}}e_2 + \gamma_{3_{33}}e_3$

Для проверки, возможно ли построение цифрового фильтра в каждой конкретной неканонической ГЧС, промоделируем построение его передаточной функции.

Пусть коэффициенты $A = a_1e_1 + a_2e_2 + a_3e_3$, $B = b_1e_1 + b_2e_2 + b_3e_3$, $C = c_1e_1 + c_2e_2 + c_3e_3$, $A, B, C \in \Gamma_{40}(e,3)$, где e - имя базиса, а «3» – размерность.

Тогда передаточная функция цифрового фильтра с представлением коэффициентов в неканонической ГЧС будет иметь вид:

$$H_{\Gamma_{40}} = \frac{(A + Bz^{-1}) \cdot \overline{(1 + Cz^{-1})}}{N(1 + Cz^{-1})} = \frac{a_1 + \frac{K}{z} + \frac{M}{z^2} + \frac{L}{z^3}}{1 + \frac{N}{z} + \frac{P}{z^2} + \frac{Q}{z^3}},$$

где N, P, Q - коэффициенты, зависящие только от c_1, c_2, c_3 , а K, M, L - коэффициенты, зависящие от $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$. При этом, если какие-либо из компонентов гиперкомплексных коэффициентов A, B, C отсутствуют, данная гиперкомплексная числовая система исключается из списка систем, удовлетворяющих критериям построения цифрового фильтра.

Рассмотрим пример реализации конкретного эллиптического фильтра низких частот третьего порядка, вещественные коэффициенты которого взяты из работы [69]. Передаточная функция с вещественными коэффициентами будет иметь вид:

$$H_3(z) = \frac{0.287589z^3 + 0.6888683z^2 + 0.6888683z + 0.287589}{z^3 + 0.418204z^2 + 0.473048z + 0.061292}. \quad (4.13)$$

Используя метод, описанный в 4.2.1, приравниваем значения при z^{-i} и находим значения гиперкомплексных коэффициентов из системы

$$\begin{cases} N = 0.418204; \\ P = 0.473048; \\ Q = 0.061292. \end{cases} \quad (4.14)$$

Выполняем проверку, имеет ли решения система (4.14), и если да, то выбранная неканоническая ГЧС может участвовать в дальнейшем синтезе и оптимизации цифрового фильтра.

Алгоритм выбора неканонических ГЧС реализован в пакете MAPLE.

4.2.3. Построение выражения для суммарной параметрической чувствительности цифрового фильтра с коэффициентами в неканонических ГЧС и ее оптимизация.

Параметрическая чувствительность цифрового фильтра представляет собой чувствительность модуля передаточной функции цифрового фильтра $|H(w)|$ к вариации коэффициентов передаточной функции фильтра [111]. Функция параметрической чувствительности позволяет провести анализ влияния погрешности коэффициентов на выходной сигнал. Для исследований фильтров с гиперкомплексными коэффициентами необходимо учитывать суммарную возможную погрешность по каждому из коэффициентов передаточной функции.

Рассмотрим неканоническую ГЧС размерности 3 изоморфную системе прямой суммы $R \oplus C$ с таблицей умножения [112-113]:

$$\Gamma_{41}(e,3) = \begin{array}{|c|c|c|} \hline e_1 & e_2 & e_3 \\ \hline e_2 & -e_1 + e_3 & -2e_2 \\ \hline e_3 & -2e_2 & 2e_1 - e_3 \\ \hline \end{array}$$

В данной таблице имеется 4 неканонические ненулевые константы, в отличие от триплексной системы, у которой их 2.

Тогда коэффициенты передаточной функции H_Γ имеют вид:

$$A = a_1 e_1 + a_2 e_2 + a_3 e_3, \quad B = b_1 e_1 + b_2 e_2 + b_3 e_3, \quad C = c_1 e_1 + c_2 e_2 + c_3 e_3, \quad A, B, C \in \Gamma_{41}(e,3) .$$

Суммарная параметрическая чувствительность фильтра первого порядка с коэффициентами в ГЧС размерности 3 будет иметь вид [67]:

$$RCS = \sum_{i=1}^9 \frac{a_i}{|H|} \cdot \frac{\partial |H|}{\partial a_i}, \quad (4.15)$$

где $\alpha_1 = a_1, \alpha_2 = a_2, \alpha_3 = a_3, \alpha_4 = b_1, \alpha_5 = b_2, \alpha_6 = b_3, \alpha_7 = c_1, \alpha_8 = c_2, \alpha_9 = c_3$.

Передаточная функция (4.13) цифрового фильтра первого порядка с гиперкомплексными коэффициентами в $\Gamma_{41}(e,3)$ будет иметь вид:

$$H_{\Gamma_{41}} = \frac{a_1 + \frac{K}{z} + \frac{M}{z^2} + \frac{L}{z^3}}{1 + \frac{N}{z} + \frac{P}{z^2} + \frac{Q}{z^3}},$$

где

$$K = a_2c_2 - a_3c_3 - 3a_1c_3 + 2a_1c_1 + b_1;$$

$$M = -2b_3c_3 + c_2a_2c_3 + c_2a_2c_1 - 3a_1c_1c_3 + c_2b_2 - 2a_3c_1c_3 + 4a_3c_3^2 + 2a_1c_2^2 + a_1c_1^2 + 2a_3c_2^2 - 3b_1c_3 + 2a_1c_3^2 + 2b_1c_1;$$

$$L = c_2b_2c_3 + b_1c_1^2 - 2b_3c_1c_3 + c_2b_2c_1 + 2b_1c_2^2 - 3b_1c_1c_3 + 2b_1c_3^2 + 2b_3c_2^2 + 4b_3c_3^2;$$

$$N = 3c_1 - 3c_2;$$

$$P = -6c_1c_3 + 3c_2^2 + 3c_1^2;$$

$$Q = 3c_1c_2^2 + 3c_2^2c_3 + c_1^3 - 3c_1^2c_3 + 4c_3^3.$$

Для получения конкретных значений коэффициентов $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$ возьмем фильтр третьего порядка с вещественными коэффициентами и передаточной функцией (4.14).

Используя метод, описанный выше, приравниваем значения при z^{-i} и находим значения гиперкомплексных коэффициентов.

Из системы

$$\begin{cases} N = 3c_1 - 3c_2 = 0.418204; \\ P = -6c_1c_3 + 3c_2^2 + 3c_1^2 = 0.473048; \\ Q = 3c_1c_2^2 + 3c_2^2c_3 + c_1^3 - 3c_1^2c_3 + 4c_3^3 = 0.061292 \end{cases}$$

Получаем значения c_i : $c_1 = 0.1403252267$, $c_2 = -0.3718209092$, $c_3 = 0.0009238933689$.

Подставляем в числитель передаточной функции и приравниваем к коэффициентам из передаточной функции вещественного фильтра:

$$\begin{cases} a_1 = 0.287589 \\ 0.2778787733a_1 - 0.3718209092a_2 - 0.001847786738a_3 + b_1 = 0.6888683 \\ -0.001847786738b_3 - 0.05251937625a_2 + 0.2958055168a_1 - 0.3718209092b_2 + \\ + 0.2762457002a_3 + 0.2778787733b_1 = 0.6888683 \\ -0.05251937625b_2 + 0.2958055168b_1 + 0.2762457002b_3 = 0.287589 \end{cases} \quad (4.16)$$

Выражаем a_1, a_2, b_1, b_3 через a_3, b_2 :

$$\begin{aligned} a_1 &= 0.287589 \\ a_2 &= 8.446312201 - 5.370129737a_3 + 7.221392887b_2 \\ b_1 &= 3.749468903 - 1.994878735a_3 + 2.685064869b_2 \\ b_3 &= -2.973890946 + 2.136127855a_3 - 2.68506487b_2 \end{aligned} \quad (4.17)$$

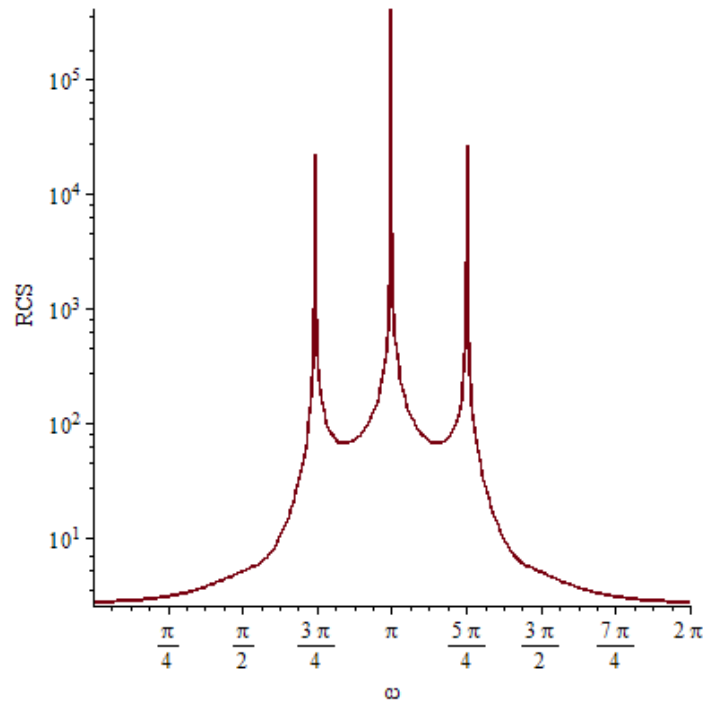


Рис. 4.5. Суммарная параметрическая чувствительность фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ при $a_3 = b_2 = 0$.

В системе (4.17) параметры a_3, b_2 могут принимать любые значения. Допустим, что $a_3 = b_2 = 0$. Тогда, получим суммарную параметрическую чувствительность для фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$, построенную по формуле (4.15). На рис. 4.5 представлен график такой суммарной параметрической чувствительности.

Сопоставленные графики суммарной параметрической чувствительности построенного фильтра с гиперкомплексными коэффициентами к суммарной параметрической чувствительности фильтра с вещественными коэффициентами, а также их отношение представлены на рис. 4.6 и рис. 4.7 соответственно.

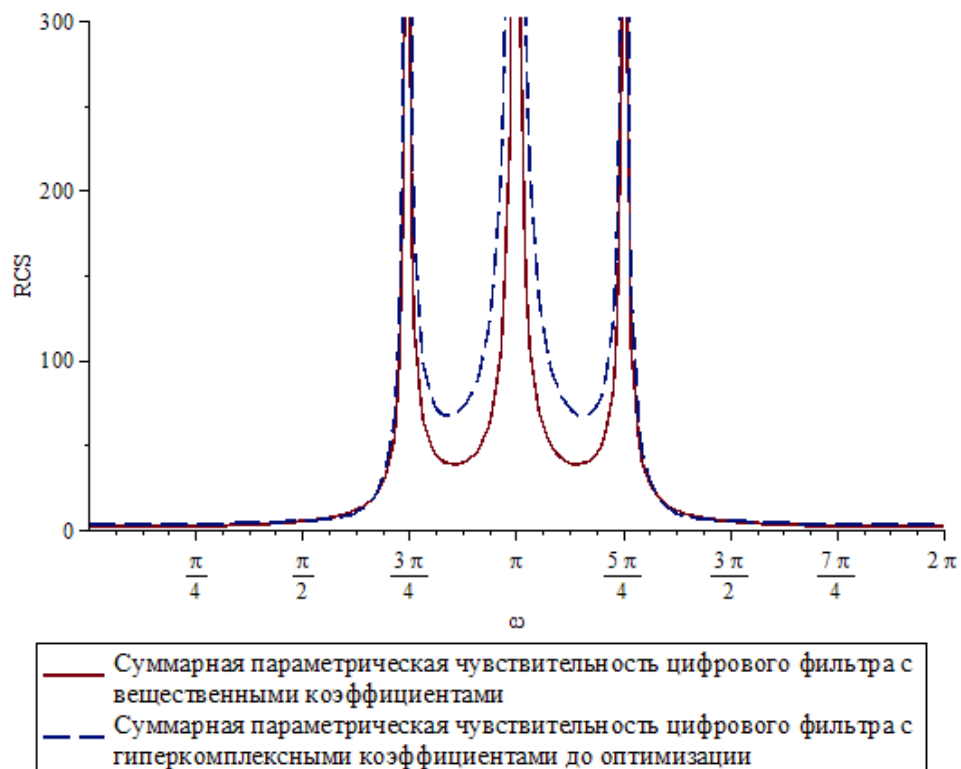


Рис. 4.6. Графики суммарных параметрических чувствительностей фильтров с вещественными и гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ при

$$a_3 = b_2 = 0.$$

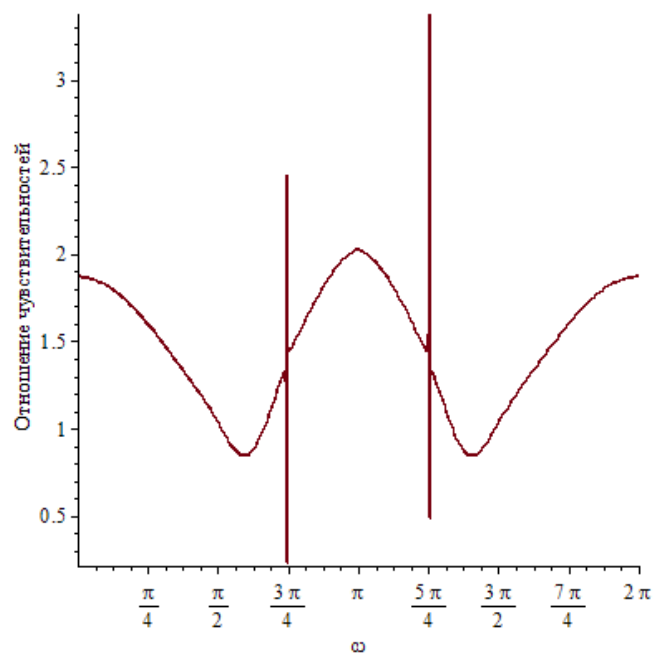


Рис. 4.7. Отношение параметрической чувствительности фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ к параметрической чувствительности фильтра с вещественными коэффициентами.

Как видим, в данном случае, чувствительность гиперкомплексного фильтра оказывается значительно выше, чем вещественного фильтра.

Параметры фильтра a_3, b_2 могут принимать различные значения без изменения передаточной функции. Этим обстоятельством можно воспользоваться для оптимизации параметрической чувствительности фильтра [112-113].

Проведем оптимизацию полученных результатов. Необходимо подобрать такие значения a_3, b_2 , чтобы удовлетворялись условия (4.17) и при этом оптимизировать некоторый критерий.

Для этого вычислим функцию суммарной чувствительности, выражая все компоненты через a_3, b_2 .

$$\begin{aligned}
 RCS_{\Gamma_{41}} = & 2.87589 \cdot 10^5 \left| (z(z^2 + 0.2778787733z + 0.2958055168)) / (6.8886829998 \cdot 10^5 z + \right. \\
 & + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^2 + 2.875889996 \cdot 10^5 - 0.000043zb_2 - 0.0001za_3 - \\
 & - 0.001z^2a_3 - 0.0004b_2) \left| + 3.718209092 \cdot 10^5 (8.4463312201 - 5.370129737a_3 + \right. \\
 & + 7.221392887b_2) \left| ((z^3 + 0.418204z^2 + 0.4730479999z + 0.061292)z) / ((z^2 + 0.2769548799z + \right. \\
 & + 0.4339283669)(6.888682998 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 2.875889996 \cdot 10^5 - \\
 & - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2) \left| + 2 \cdot 10^6 a_3 \left| z(0.0009238933689z - \right. \right. \\
 & - 0.1381228502) / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 2.875889 \cdot 10^5 - \\
 & - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2) \left| + 10^6 (3.749468903 - 1.994878735a_3 + \right. \\
 & + 2.685064869b_2) \left| z^2 + 0.2778787733z + 0.2958055168) / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + \right. \\
 & + 2.87589 \cdot 10^5 z^3 + 2.87589 \cdot 10^5 - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2) \left| + \right. \\
 & + 3.718209092 \cdot 10^5 b_2 \left| (z^3 + 0.418204z^2 + 0.4730479999z + 0.061292) / ((z^2 + 0.2769548799z + \right. \\
 & + 0.4339283669)(6.888682998 \cdot 10^5 z^2 + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 2.875889996 \cdot 10^5 - \\
 & - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2) \left| + 2 \cdot 10^6 (-2.973890946 + 2.136127855a_3 - \right. \\
 & - 2.68506487b_2) \left| (0.0009238933689z + 0.1381228502) / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + \right. \\
 & + 2.87589 \cdot 10^5 z^3 + 2.87589 \cdot 10^5 - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2) \left| + \right. \\
 & + 1.403252267 \cdot 10^5 \left| (0.20109286z + 0.8080145342z^2 + 0.3967868515z^3 - 0.07118465934 + \right. \\
 & + 2.685064869z^4b_2 - 1.994878735z^4a_3 + 1.502167918z^3b_2 - 1.39254783z^3a_3 + \\
 & - 0.3439826239zb_2 + 1.428773891z^2b_2 - 1.177148979z^2a_3 - 0.3863640851za_3 - 0.287589z^5 + \\
 & - 2.371732304^4 - 0.0342181936a_3 + 0.023245791b_2) / ((6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + \\
 & + 2.87589 \cdot 10^5 z^3 + 2.87589 \cdot 10^5 - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2)(z^3 + \\
 & - 0.488204z^2 + 0.473048z + 0.061292)) \left| - 3.71820992 \cdot 10^5 \left| ((3.899734973z + 2.553110588z^2 + \right. \right.
 \end{aligned}$$

$$\begin{aligned}
& + 0.9985997616 + 8.446312201z^3 - 5.370129737z^3a_3 + 3z^2b_2 - 0.6453745599a_3 + 0.439283673b_2) \cdot \\
& \cdot (z^3 + 8.446312201z^3 - 5.370129737z^3a_3 + 3z^2b_2 - 0.6453745599a_3 + 0.439283673b_2)(z^3 + \\
& + 0.418204z^2 + 0.473048z + 0.061292)) / ((z^2 + 0.2769548799z + 0.4339283669)^2 \cdot \\
& \cdot (6.888682998 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 2.875889996 \cdot 10^5 - 0.000043zb_2 - \\
& - 0.0001za_3 - 0.001z^2a_3 - 0.0004b_2)) | + 1847.786738 | (-0.4416591322z - 1.609719097z^2 - \\
& - 1.098032331z^3 - 0.0741899487 - 2.685064868z^4b_2 + 1.299719855z^4a_3 - 1.502167918z^3b_2 + \\
& + 0.3697478256z^3a_3 - z^5a_3 - 0.3439826232zb_2 - 1.42877389z^2b_2 + 0.8033734483z^2a_3 + \\
& + 0.1641200202za_3 - 3.306608615z^4 + 0.0076218562a_3 - 0.0232457908b_2) / ((6.8886823 \cdot 10^5 z + \\
& + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 2.875889 \cdot 10^5 - 0.000043zb_2 - 0.0001za_3 - 0.001z^2a_3 - \\
& - 0.0004b_2)(z^3 + 0.418204z^2 + 0.473048z + 0.06129)) |
\end{aligned}$$

Поскольку функция параметрической чувствительности положительна на всем отрезке $\omega = 0..2\pi$, то в качестве критерия можно взять сумму значений функции параметрической чувствительности от параметров a_3, b_2 на некоторой совокупности значений ω . Выделим на отрезке $\{0..2\pi\}$ 33 равномерно расположенные точки и вычислим значения функции в каждой точке с учетом того, что $z = \sin(\omega) + i \cdot \cos(\omega)$. Затем производится минимизация суммы этих

$$\text{значений } S_{RCS_{\Gamma_{41}}}(\omega, a_3, b_2) = \sum_{i=0}^{32} RCS(a_3, b_2, \omega_i).$$

Привести в данной работе функцию $S_{RCS_{\Gamma_{41}}}(\omega, a_3, b_2)$ не представляется возможным, так как она слишком громоздкая. Также неудачной оказалась попытка дифференцирования такой функции по компонентам a_3, b_2 . Поэтому ее оптимизация представляет собой серьезную самостоятельную задачу. Для доказательства работоспособности излагаемого метода достаточно найти приближенный оптимум, что можно выполнить построением трехмерного графика функции $S_{RCS_{\Gamma_{41}}}(\omega, a_3, b_2)$, для чего использовались процедуры система аналитических вычислений MAPLE. При этом возможна многоступенчатая процедура: сначала выбирается широкая область поиска, потом она сужается. Соответственно на рис. 4.8. представлена широкая область поиска, на рис. 4.9. – суженная.

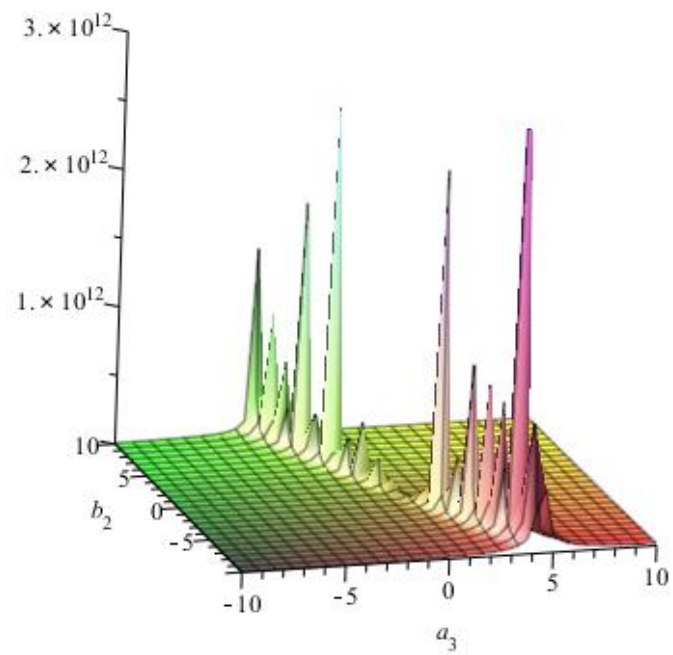


Рис. 4.8. График $S_{RCS\Gamma_{41}}(\omega, a_3, b_2)$ для $a_3 \in \{-10..10\}, b_2 \in \{-10..10\}$.

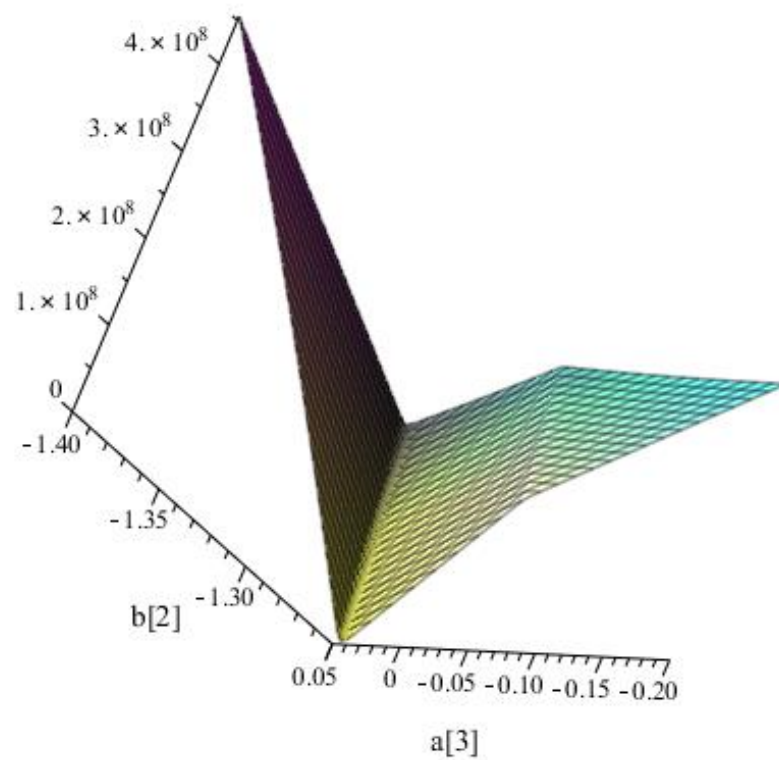


Рис. 4.9. График $S_{RCS\Gamma_{41}}(\omega, a_3, b_2)$ для $a_3 \in \{-0.25..0.05\}, b_2 \in \{-1.4..-1.25\}$.

Промоделируем функцию суммарной чувствительности для одного из полученных локальных минимумов при $a_3 = -0.2316615, b_2 = -1.2783899677$ (рис. 4.10).

Соотношение чувствительности фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ к чувствительности вещественного фильтра показано на рис. 4.11. А рис. 4.12 иллюстрирует сопоставленные графики чувствительностей фильтров с вещественными и гиперкомплексными коэффициентами до и после оптимизации.

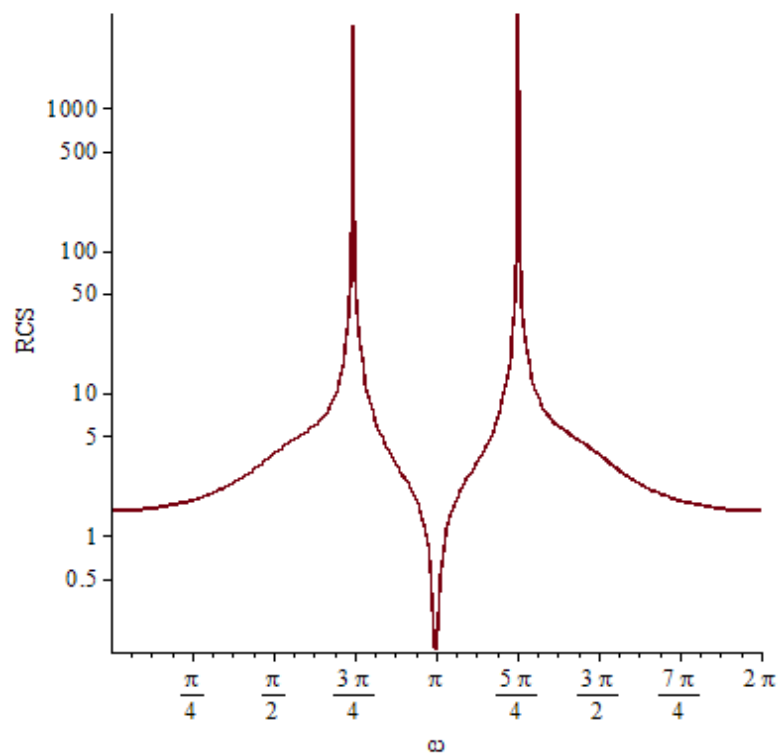


Рис. 4.10. Суммарная параметрическая чувствительность фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ после оптимизации.

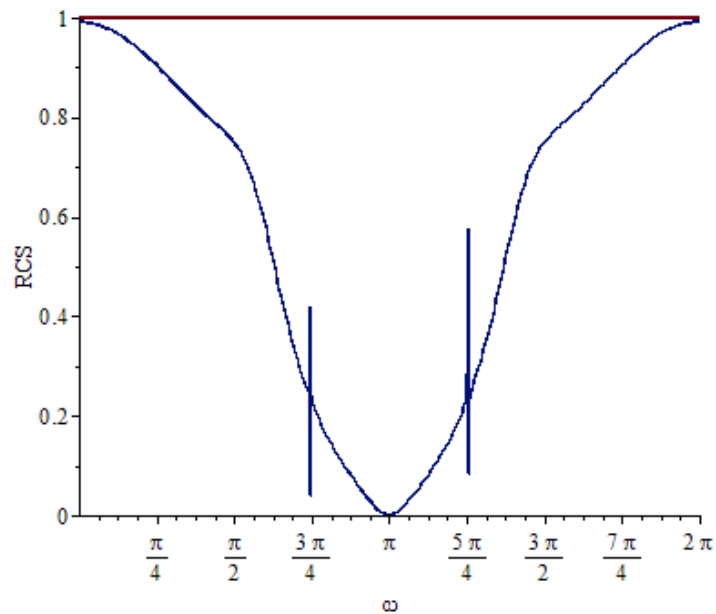


Рис. 4.11. Соотношение чувствительности фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ к чувствительности фильтра с вещественными коэффициентами.

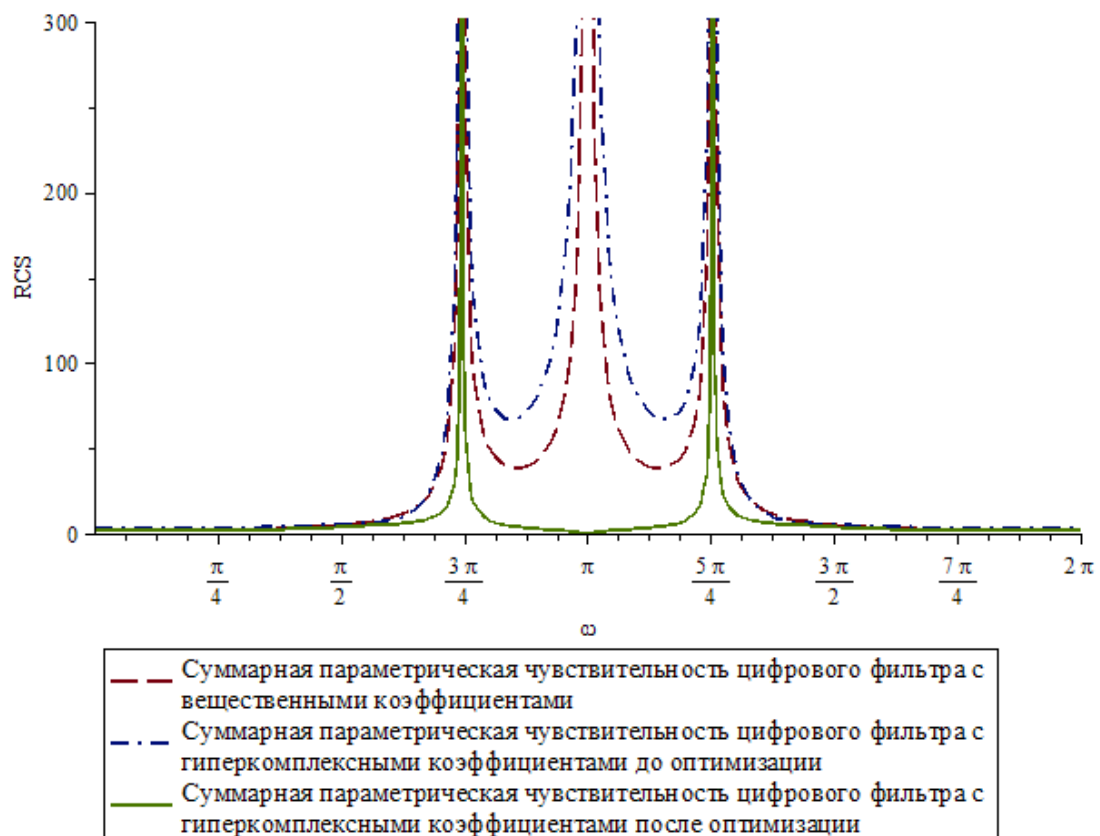


Рис. 4.12. Сопоставленные графики чувствительностей фильтров с вещественными коэффициентами и гиперкомплексными коэффициентами в системе $\Gamma_{41}(e,3)$ до и после оптимизации.

Рассмотрим другую неканоническую ГЧС [113].

$$\Gamma_{42}(e,3)$$

e_1	e_2	e_3
e_2	$-2e_1 - 3e_2$	$-e_3$
e_3	$-e_3$	$-8e_1 - 4e_2$

Данная система также изоморфна системе прямой суммы $R \oplus C$, оператор изоморфизма выглядит следующим образом:

$$\begin{cases} e_1 = E_1 + E_2; \\ e_2 = 2E_1 - E_2; \\ e_3 = 2E_3. \end{cases}$$

Передаточная функция (4.13) цифрового фильтра первого порядка с гиперкомплексными коэффициентами в $\Gamma_{42}(e,3)$ будет иметь вид:

$$H_{\Gamma} = \frac{a_1 + \frac{K}{z} + \frac{M}{z^2} + \frac{L}{z^3}}{1 + \frac{N}{z} + \frac{P}{z^2} + \frac{Q}{z^3}},$$

где

$$K = 2a_2c_2 + 8a_3c_3 - 4a_1c_2 + 2a_1c_1 + b_1;$$

$$M = 8a_2c_3^2 + 2a_2c_1c_2 + 8b_3c_3 - 4a_1c_3^2 - 4b_1c_2 + 2b_1c_1 + 2b_2c_2 + 3a_1c_2^2 + a_1c_1^2 - 4a_1c_1c_2 - 16a_3c_2c_3 + 8a_3c_1c_3;$$

$$L = b_1c_1^2 - 16b_3c_2c_3 + 2b_2c_1c_2 - 2b_2c_2^2 - 4b_1c_1c_2 + 8b_3c_1c_3 + 3b_1c_2^2 + 8b_2c_3^2 - 4b_1c_3^2;$$

$$T = 3c_1 - 4c_2;$$

$$P = 5c_2^2 + 4c_3^2 - 8c_1c_3 + 3c_1^2;$$

$$Q = 5c_1c_2^2 - 4c_1^2c_2 + c_1^3 + 4c_1c_3^2 - 8c_2c_3^2 - 2c_2^3.$$

Аналогично предыдущему примеру, вычислим значения коэффициентов $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$. Для начала формируем систему на основе приравнивая коэффициентов при z^{-i} в знаменателе.

$$\begin{cases} T = 3c_1 - 4c_2 = 0.418204; \\ P = 5c_2^2 + 4c_3^2 - 8c_1c_3 + 3c_1^2 = 0.473048; \\ Q = 5c_1c_2^2 - 4c_1^2c_2 + c_1^3 + 4c_1c_3^2 - 8c_2c_3^2 - 2c_2^3 = 0.061292, \end{cases}$$

откуда

$$\begin{aligned} c_1 &= 0.1357057599, \\ c_2 &= -0.02771680107, \\ c_3 &= -0.0322006353. \end{aligned}$$

Подставляем в числитель передаточной функции и приравниваем к коэффициентам из передаточной функции вещественного фильтра:

$$\begin{cases} a_1 = 0.287589 \\ 0.282498242a_1 - 0.005543360214a_2 - 2.576050824a_3 + b_1 = 0.6888683 \\ -2.576050824b_3 + 0.8287371009a_2 - 0.3948087339a_1 - 0.005543360214b_2 + \\ -0.3638649122a_3 + 0.2824982402b_1 = 0.6888683 \\ 0.8287371009b_2 - 0.3948087339b_1 - 0.3638649122b_3 = 0.287589 \end{cases} \quad (4.18)$$

Выражаем a_1, a_2, a_3, b_2 через b_1, b_3 :

$$\begin{aligned} a_1 &= 0.287589 \\ a_2 &= 0.8617832604 - 0.1670945344b_1 + 3.108405333b_3 \\ a_3 &= -0.2377384865 + 0.3885506667b_1 - 0.006688924881b_3 \\ b_2 &= 0.3270207858 + 0.4763980440b_1 + 0.4390595182b_3 \end{aligned}$$

В системе (4.18) параметры b_1, b_3 могут принимать любые значения. Допустим, что $b_1 = b_3 = 0$. Тогда, получим суммарную параметрическую чувствительность для фильтра с гиперкомплексными коэффициентами, построенную по формуле (4.15) (рис. 4.13).

График отношения суммарной параметрической чувствительности построенного фильтра с гиперкомплексными коэффициентами в системе к суммарной параметрической чувствительности фильтра с вещественными коэффициентами представлен на рис. 4.14, а на рис 4.15 представлены графики чувствительностей фильтров с вещественными и гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$.

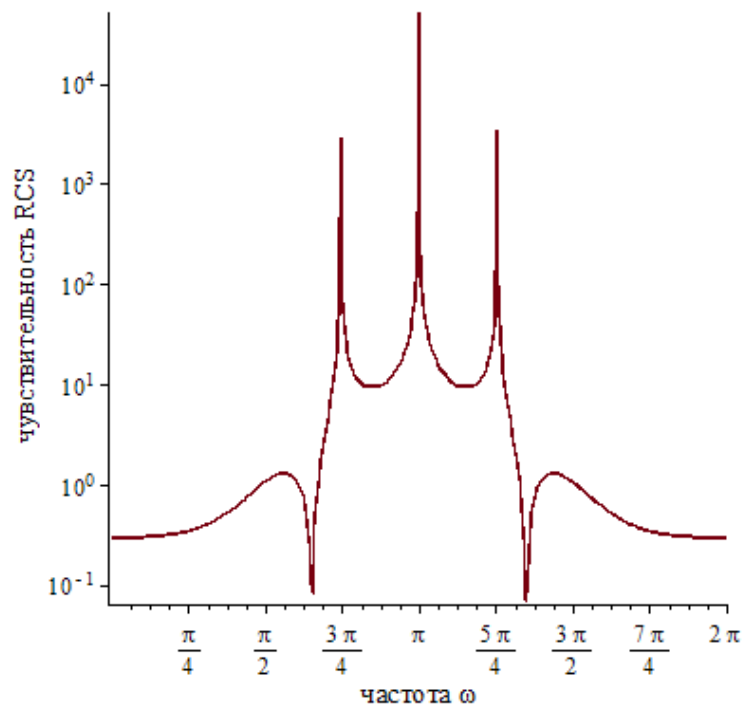


Рис. 4.13. Суммарная параметрическая чувствительность фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$.

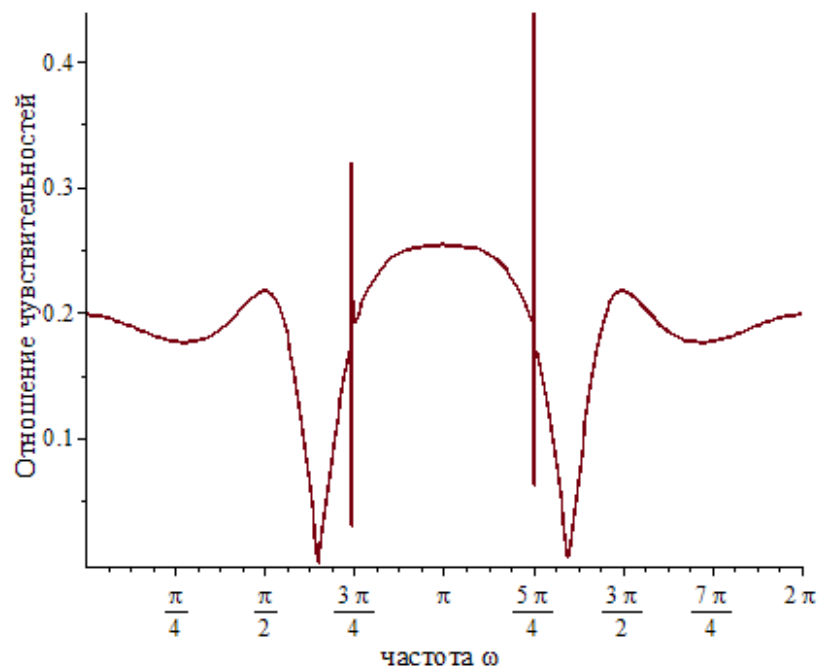


Рис. 4.13. Отношение суммарных параметрических чувствительностей фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ и фильтра с вещественными коэффициентами.

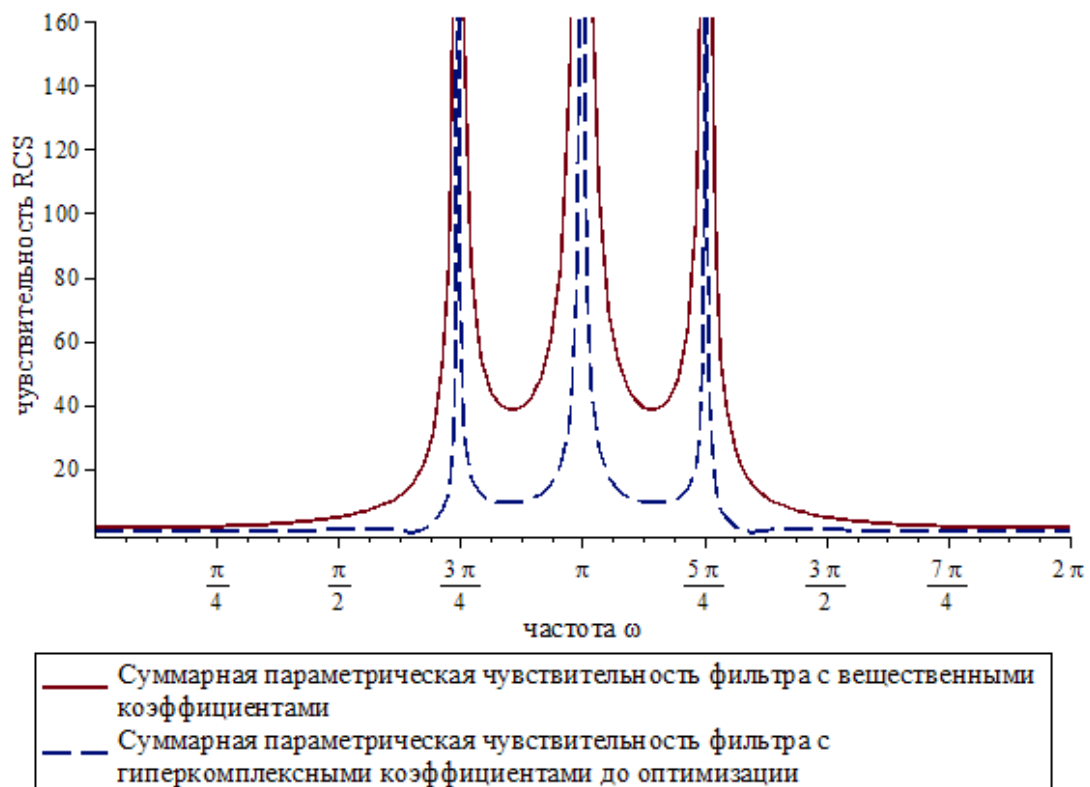


Рис. 4.15. Сопоставленные графики суммарной параметрической чувствительности фильтров с вещественными коэффициентами и гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$.

Как видим, суммарная чувствительность гиперкомплексного фильтра в данном случае ниже, чем суммарная чувствительность вещественного фильтра. Тем не менее, параметрическая чувствительность гиперкомплексного фильтра является высокой для некоторых значений ω .

Однако, в соответствии с [114], есть возможность дальнейшей минимизации параметрической чувствительности фильтра. Выразим компоненты функции параметрической чувствительности для системы $\Gamma_{42}(e,3)$ через b_1, b_3 .

$$\begin{aligned}
 RCS_{\Gamma_{41}} = & 2.87589 \cdot 10^5 \left| (z(z^2 + 0.2824982402z - 0.3948087339)) / (6.888683 \cdot 10^5 z + \right. \\
 & + 6.888683 \cdot 10^5 z^2 + 287589 \cdot 10^5 z^3 + 0.000065 z b_3 + 287589 \cdot 10^5 + 0.000194 z^2 b_1 - 0.0001 b_1) \left| + \right. \\
 & + 179.2(0.8661732604 + 3.108405330 b_3 - 0.1670945344 b_1) \left| (-30.93392977 z + 4624.649) z / \right. \\
 & / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065 z b_3 + 2.87589 \cdot 10^5 + \\
 & + 0.000194 z^2 b_1 - 0.0001 b_1) \left| + 2.576050824 \cdot 10^6 (-0.2377384865 - 0.006688924881 b_3 + \right.
 \end{aligned}$$

$$\begin{aligned}
& + 0.3885506667b_1) \left| ((z^3 + 0.4182040001z^2 + 0.473048z + 0.061292)z) / ((z^2 + 0.27695488z + \right. \\
& + 0.4339283668)(6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + \\
& + 2.87589 \cdot 10^5 + 0.00194z^2b_1 - 0.0001b_1)) \left| + 10^6 b_1 \left| (z^2 + 0.2824982402z - 0.3948087339) / \right. \right. \\
& / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + 2.87589 \cdot 10^5 + \\
& + 0.00194z^2b_1 - 0.0001b_1) \left| + 179.2(0.3470207858 + 0.476398044b_1 + 0.4390595182b_3) \cdot \right. \\
& \left. |(-30.93392977z + 4624.649) / (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + \right. \\
& + 0.000065zb_3 + 2.87589 \cdot 10^5 + 0.00194z^2b_1 - 0.0001b_1) \left| + 2.576050824 \cdot 10^6 b_3 \left| (z^3 + \right. \right. \\
& + 0.418204001z^2 + 0.473048001z + 0.06129200005) / ((z^2 + 0.27695488z + 0.4339283668) \cdot \\
& \cdot (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + 2.87589 \cdot 10^5 + \\
& + 0.00194z^2b_1 - 0.0001b_1)) \left| + 1.357057599 \cdot 10^5 \left| (-0.5250973802z - 1.40449263z^2 - \right. \right. \\
& - 2.220572639z^3 - 1.078332612z^2b_3 - 0.1361613063 + 10^{-11} z^4b_3 - 2.578484692b_3z^3 + \\
& + 0.6980613945z^3b_1 - 0.287589z^5 - 1.3777366z^4 + z^4b_1 - 1.219747025zb_3 + \\
& + 0.5900854807z^2b_1 + 0.1936779808zb_1 + 0.01715301943b_1 - 0.1580404834b_3) / \\
& / ((6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + 2.87589 \cdot 10^5 + \\
& + 0.00194z^2b_1 - 0.0001b_1)(z^3 + 0.418204z^2 + 0.473048z + 0.061292)) \left| - 5543.360214 \cdot \right. \\
& \cdot \left| (0.4819770815z + 1.203657431z^2 + 1.984835137z^3 + 1.70101216z^2b_3 + 0.1334225252 - \right. \\
& - 0.1670945344z^5b_1 + 3.108405333z^5b_3 + 2.160835571z^4b_3 + 4.46851934z^3b_3 - \\
& - 0.519934988z^3b_1 + 0.8661732604z^5 + 1.436021731z^4 - 0.6161572493z^4b_1 + \\
& + 1.300698148zb_3 - 0.3574985891z^2b_1 - 1.339747589zb_1 - 0.01302061233b_1 + \\
& + 0.1616924388b_3) / ((6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + \\
& + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + 2.87589 \cdot 10^5 + 0.00194z^2b_1 - 0.0001b_1)(z^3 + \\
& + 0.418204z^2 + 0.473048z + 0.061292)) \left| - 2.576050824 \cdot 10^6 \left| ((z^3 + 0.418204z^2 + \right. \right. \\
& + 0.473048z + 0.061292)(-0.1810409257 - 0.4384584492z^2 - 0.2377384865z^3 - \\
& - 1.00370506z^2b_3 - 0.03094774081 - 0.006688924881b_3z^3 + +0.3885506661z^3b_1 - \\
& - 0.2803704614zb_3 + 0.2152220066z^2b_1 + 0.1984065488zb_1 + 0.04669546693b_1 - \\
& - 0.4347322325b_3) / ((z^2 + 0.27695488z + 0.433928367)^2 (6.888683 \cdot 10^5 z + 6.888683 \cdot 10^5 z^2 + \\
& + 2.87589 \cdot 10^5 z^3 + 0.000065zb_3 + 2.87589 \cdot 10^5 + 0.00194z^2b_1 - 0.0001b_1)) \left| \right.
\end{aligned}$$

Аналогично предыдущему примеру, выделим на отрезке $\{0..2\pi\}$ 33 равноотдаленных точки для вычисления значения функции в каждой точке с учетом того, что $z = \sin(\omega) + i \cdot \cos(\omega)$. Поскольку полученная функция $S_{RCS_{\Gamma_{41}}}(\omega, b_1, b_3)$ не дифференцируема и громоздкая, воспользуемся графическим методом для поиска локальных минимумов. На рис 4.16 показана широкая область поиска, на рис 4.17 – узкая.

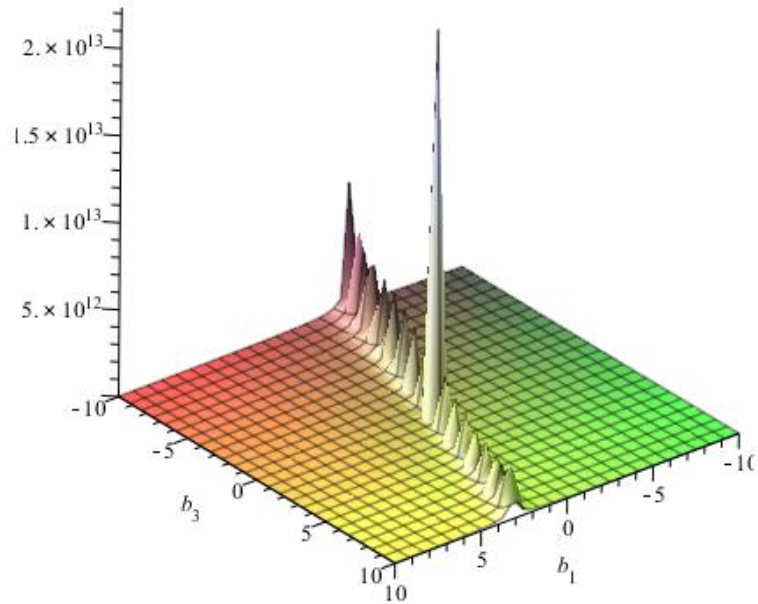


Рис. 4.16. График $S_{RCS\Gamma_{42}}(\omega, b_1, b_3)$ для широкой области поиска;
 $b_1 \in \{-10..10\}, b_3 \in \{-10..-10\}$.

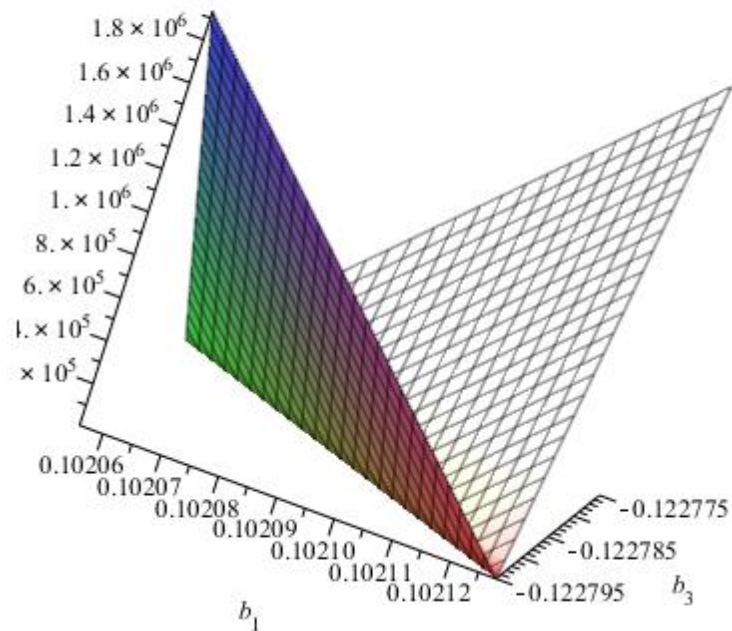


Рис. 4.17. График $S_{RCS\Gamma_{42}}(\omega, b_1, b_3)$ для суженной области
поиска; $b_1 \in \{0.102056..0.102128\}, b_3 \in \{-0.122795..-0.122775\}$.

На рис. 4.18 представлен график изменений параметрической чувствительности вблизи одного из локальных минимумов при $b_1 = 0.102056, b_3 = -0.122795$.

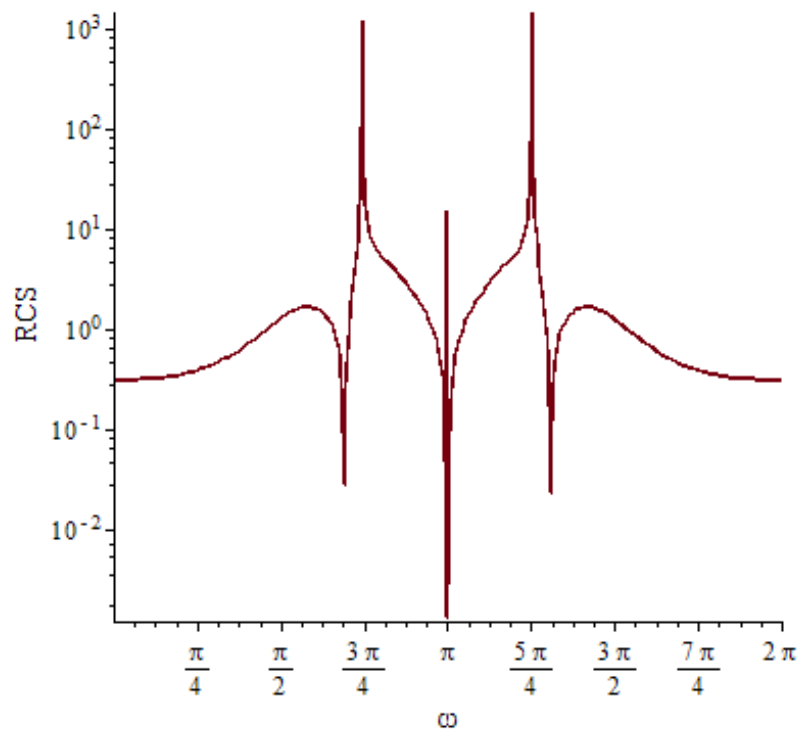


Рис. 4.18. Суммарная параметрическая чувствительность фильтра с гиперкомплексными коэффициентами после оптимизации.

Отношение чувствительности фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ после оптимизации к чувствительности фильтра с вещественными коэффициентами показано на рис. 4.19, а на рис. 4.20 – сопоставленные графики чувствительностей фильтров с вещественными коэффициентами и гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ до и после оптимизации. В целом, параметрическая чувствительность полученного фильтра с гиперкомплексными коэффициентами после оптимизации значительно ниже, чем чувствительность полученная до оптимизации [115].

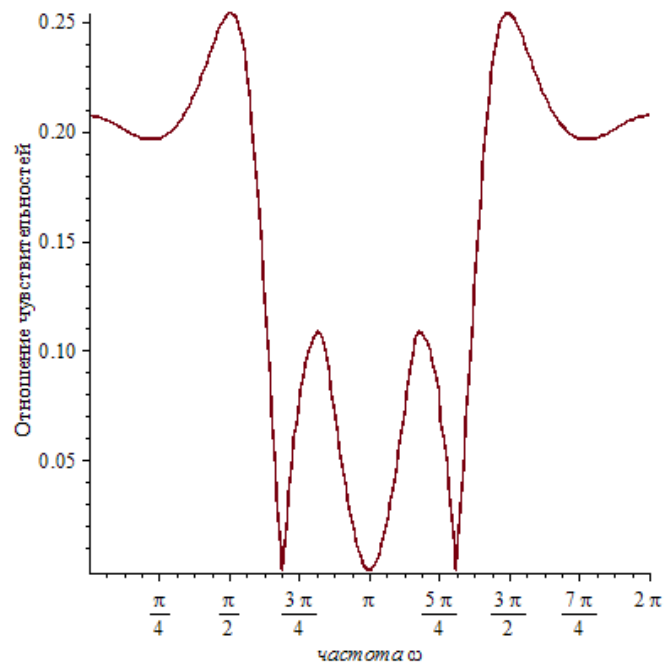


Рис. 4.19. Отношение суммарной параметрической чувствительности фильтра с гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ к чувствительности вещественного фильтра.

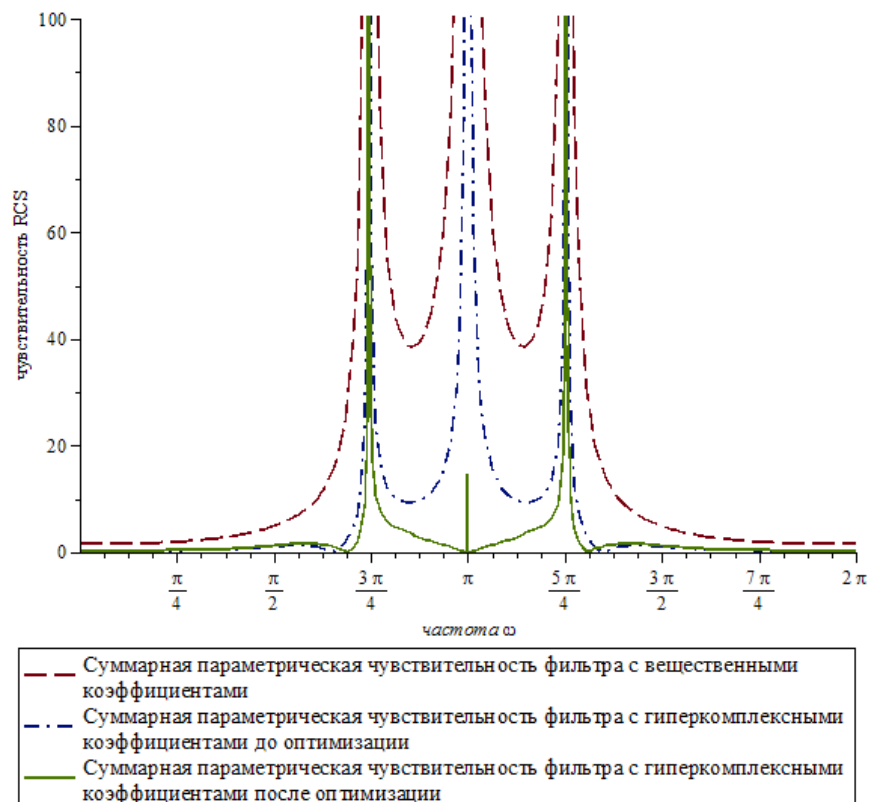


Рис. 4.20. Сопоставленные графики чувствительностей фильтров с вещественными коэффициентами и гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ до и после оптимизации.

Если же рассмотреть отношение чувствительностей фильтра с гиперкомплексными коэффициентами до и после оптимизации (рис. 4.21), то можно увидеть, что при $b_1 = 0.102056, b_3 = -0.122795$ суммарная параметрическая чувствительность гиперкомплексного фильтра будет ниже для $\omega \in \{\frac{5\pi}{8} .. \frac{11\pi}{8}\}$, а при значениях $b_1 = 0, b_3 = 0$ суммарная параметрическая чувствительность будет ниже для отрезков $\omega \in \{0 .. \frac{5\pi}{8}\}, \{\frac{11\pi}{8} .. 2\pi\}$.

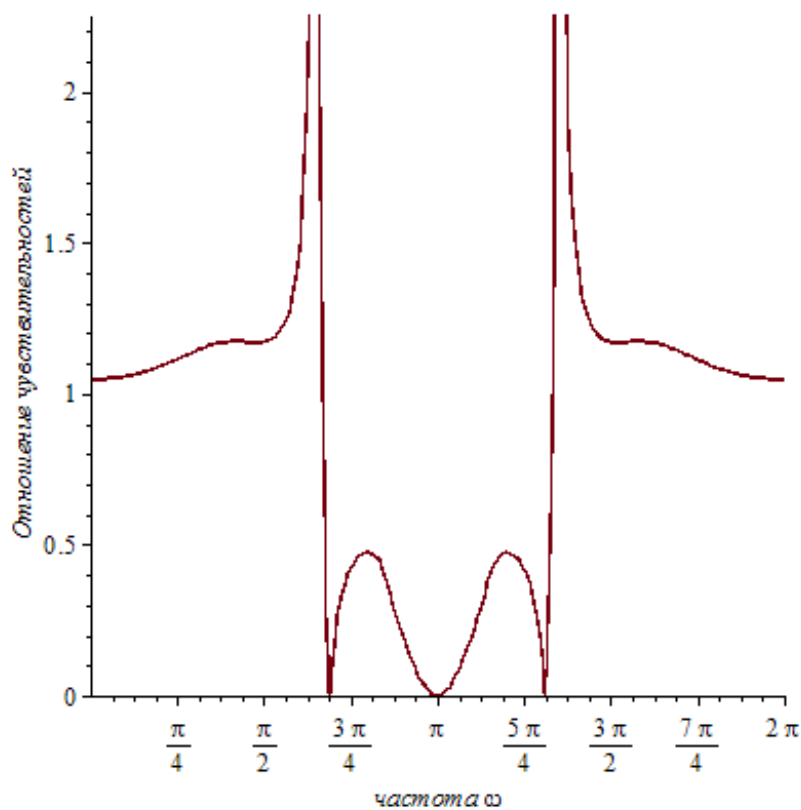


Рис. 4.21. Отношение чувствительностей фильтров с гиперкомплексными коэффициентами в системе $\Gamma_{42}(e,3)$ до и после оптимизации.

Таблица 4.5. Изменение суммарной параметрической чувствительности фильтра с коэффициентами в неканонических ГЧС.

Суммарные параметрические чувствительности фильтров RCS	Усредненное изменение, %
---	--------------------------

RCS фильтра с вещественными коэффициентами и фильтра с коэффициентами в ГЧС $\Gamma_{41}(e,3)$ до оптимизации	+63%
RCS фильтра с вещественными коэффициентами и фильтра с коэффициентами в ГЧС $\Gamma_{41}(e,3)$ после оптимизации	-43%
RCS фильтра с вещественными коэффициентами и фильтра с коэффициентами в ГЧС $\Gamma_{42}(e,3)$ до оптимизации	-47%
RCS фильтра с вещественными коэффициентами и фильтра с коэффициентами в ГЧС $\Gamma_{42}(e,3)$ после оптимизации	-51%

В таблице 4.5 показано усредненное изменение параметрической чувствительности фильтра с коэффициентами в неканонических ГЧС по сравнению с фильтром с вещественными коэффициентами, вычисленное с помощью функции критерия оптимальности. По сравнению с известными работами по оптимизации параметрической чувствительности в фильтрах с гиперкомплексными коэффициентами [35-37, 65-72], получим максимальное уменьшение чувствительности до 40%. Возможна дальнейшая оптимизация параметрической чувствительности путем поиска и анализа других неканонических ГЧС.

Выводы по разделу 4

Рассмотрены вопросы практического применения неканонических гиперкомплексных числовых систем. Среди практических приложений выделены задачи обработки данных, представленных в неканонических гиперкомплексных числовых системах, а именно задача разделения секрета и оптимизации параметрической чувствительности цифрового фильтра.

Усовершенствована модель задачи разделения секрета в неканонических гиперкомплексных числах 3-й и 4-й размерности с восстановлением секрета с помощью алгоритма Евклида.

Показана возможность повышения стойкости задачи разделения секрета путем использования неканонической гиперкомплексной числовой системы со сложной структурой таблицы умножения, или же уменьшить количество операций для выполнения работы модели схемы разделения секрета при обеспечении такой же криптостойкости.

Сопоставлены данные о количестве вычислений для подбора ГЧС злоумышленником в случае использования канонических и неканонических гиперкомплексных числовых систем. Использование неканонической ГЧС размерности 3 для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 4, не дает нужного эффекта по минимизации вычислений, так как количество операций увеличивается в среднем на 92%. Но при использовании неканонической ГЧС размерности 4 с 9 составными ячейками в таблице умножения с коэффициентами из диапазона $\{-4,4\}$, для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 6, количество требуемых вычислений уменьшается в среднем на 44%. Следовательно можно утверждать, что использование неканонических гиперкомплексных числовых систем размерности 4 и выше в задаче разделения секрета более эффективно, чем повышение размерности канонической гиперкомплексной числовой системы. Применение неканонических ГЧС к данной модели позволяет использовать

меньшую размерность в зависимости от выбора констант при структурных единицах в таблице умножения системы, для обеспечения такой же криптостойкости, как с использованием канонических ГЧС. Показано, что для уменьшения операций при восстановлении секрета в неканонических ГЧС необходимо использовать системы без делителей нуля.

Показана возможность построения цифрового рекурсивного фильтра для неканонических гиперкомплексных числовых систем. Предложен метод синтеза неканонических гиперкомплексных числовых систем, которые удовлетворяют условиям построения цифрового фильтра с гиперкомплексными коэффициентами.

Получены выражения для определения суммарной параметрической чувствительности фильтра с гиперкомплексными коэффициентами в неканонической ГЧС. Показано, что в некоторых неканонических ГЧС параметрическая чувствительность фильтра с гиперкомплексными коэффициентами значительно ниже, чем фильтра с вещественными коэффициентами. Показано, что для других неканонических ГЧС, возможна оптимизация суммарной параметрической чувствительности цифрового фильтра.

Предложен и реализован метод оптимизации суммарной параметрической чувствительности цифрового фильтра и показаны результаты такой оптимизации для некоторых неканонических ГЧС. Показано, что возможно уменьшить суммарную параметрическую чувствительность цифровых фильтров с коэффициентами представленными неканоническими гиперчислами в выбранных системах до 50% по сравнению с чувствительностью фильтра с вещественными коэффициентами. Если сравнивать существующие модели фильтров с гиперкомплексными коэффициентами, то возможно получить уменьшение суммарной параметрической чувствительности до 41% в зависимости от выбранной системы.

ВЫВОДЫ

Представление и обработка информации с использованием гиперкомплексных числовых систем привлекало и привлекает внимание многих ученых и практиков. Использование гиперкомплексных числовых систем для математического моделирования прикладных задач требует как развития теоретических аспектов, имеющих самостоятельное значение, так и развития методов их применений в широком спектре приложений.

В работе особое внимание уделено неканоническим гиперкомплексным числовым системам, применение которых дает возможность получить более эффективное решение некоторых практических задач. Важно подчеркнуть, что и канонические и неканонические гиперкомплексные числовые системы имеют свои преимущества и практические приложения, в которых применения и тех и других систем дает наилучшие результаты.

В диссертационной работе решена научно-техническая задача разработки методов и способов представления и обработки данных в неканонических гиперкомплексных числовых системах, которые имеют большую заполненность таблиц умножения, что позволяет строить более эффективные математические модели: задачи разделения секрета с целью уменьшения количества вычислений и цифрового рекурсивного фильтра с целью его оптимизации по параметрической чувствительности.

Получены такие научные и практические результаты:

1. Усовершенствованы методы построения структур ГЧС заданной размерности в общем и частных видах, которые отличаются от существующих тем, что структурно учитывают заданные ограничения представления данных в неканонических ГЧС для моделирования практических задач, что приводит к снижению количества вычислений при построении таких структур.

2. Предложен метод построения классов изоморфизма для неканонических ГЧС размерности 2. Изоморфные системы используются для минимизации вычислений при таком представлении данных.
3. Усовершенствованы методы определения основных характеристик неканонических ГЧС и выполнения операций в таких системах, которые используются при моделировании практических задач. Впервые предложен и разработан метод вычисления вычетов в неканонических ГЧС, применимый при моделировании задачи разделения секрета и учитывает структурные особенности неканонических ГЧС.
4. Предложена и реализована модификация модулярной схемы разделения секрета, которая отличается от существующей представлением информации остатками в неканонических ГЧС по совокупности неканонических гиперкомплексных модулей, что привело к уменьшению количества вычислений и повышению стойкости. При использовании неканонической ГЧС размерности 4, для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 6, количество требуемых вычислений уменьшается в среднем на 44%.
5. Разработан метод синтеза неканонических ГЧС, удовлетворяющих критериям построения цифрового фильтра. Создана математическая модель рекурсивного цифрового фильтра с гиперкомплексными коэффициентами в полученных неканонических ГЧС третьей размерности.
6. Реализован метод оптимизации суммарной параметрической чувствительности фильтра, построенного с использованием неканонических ГЧС, что позволило существенно уменьшить параметрическую чувствительность эквивалентного фильтра с вещественными коэффициентами (до ~50%) и существующих фильтров с гиперкомплексными коэффициентами (до ~40%).
7. Расширен аналитически-программный инструментарий в системе MAPLE, который реализует предложенные модели и методы с учетом особенностей неканонических ГЧС, а именно: определение основных свойств и

выполнение операций над неканоническими гиперкомплексными числами; выполнение модулярных операций над неканоническими гиперкомплексными числами; построение структур неканонических ГЧС согласно заданным критериям; определение множества неканонических ГЧС для представления коэффициентов цифрового фильтра; реализация модели задачи разделения секрета в неканонических ГЧС.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Курош А.Г. Лекции по общей алгебре / Курош А.Г. // Москва: Наука, 1973. — 400с.
2. Кострикин А.И. Введение в алгебру / Кострикин А.И. // Москва: Наука, 1977. — 496с.
3. Общая алгебра / Мельников О.В., Ремесленников В.Н., Романьков В.А., Скорняков Л.А., Шестаков И.П. // М.: Наука, 1990. —Т.1. —591с.
4. Гиперкомплексные числовые системы и быстрые алгоритмы цифровой обработки информации / Я.А. Калиновский, Д.В. Ландэ, Ю.Е. Бояринова, Я.В. Хицко. // Киев: ИПРИ НАН Украины, 2014. – 130 с.
5. J. Keller Quaternionic, complex, duplex and real Clifford Algebras. / J. Keller // Advances in Applied Clifford Algebras. — 1994. — Vol. 4, No. 1. — P. 12.
6. P. Lounesto Octonions and Triality / P. Lounesto // Advances in Applied Clifford Algebras. —2001. — Vol. 11, No. 2 . — P. 191-213.
7. Three-Dimensional Associative Unital Algebras / P. Arezina, S. Caldwell, J. Davis, R. Frederick, G. Julius, M. Ringel // Journal of the PGSS. Mathematics Team Project P. 227-237.
8. Н. Р. Petersson The Classification of Two-dimensional. Nonassociative Algebras [Электронный ресурс] / Н. Р. Petersson. — Режим доступа: www.fernuni-hagen.de/MATHEMATIK/ALGGEO/Petersson/Separata/nonalgw. - P.35.
9. Y. Tian. Similarity and Consimilarity of Elements in the real Cayley-Dickson Algebras / Y. Tian. // Advances in Applied Clifford Algebras . —1999. — Vol. 9, No. 2 . — P. 61-76.
10. R. M. Yamaleev. Complex Algebras on n-Order Polynomials and Generalizations of Trigonometry, Oscillator Model and Hamilton Dynamics / R. M. Yamaleev //Advances in Applied Clifford Algebras. —2005. — Vol. 15, No. 1. — P. 123-150.

11. Приходовский М.А. Применение многомерных матриц для исследования гиперкомплексных чисел и конечномерных алгебр [Электронный ресурс] / Приходовский М.А.. // Режим доступа: physics.nad.ru/matboard/themes/16127.htm. - С.4.
12. G. Moreno The zero divisors of the Cayley-Dickson algebras over the real numbers [Электронный ресурс] / G. Moreno // Режим доступа: arXiv:q-alg/9710013 v1 8 Oct 1997. - P.31.
13. M. Schweitzer Zero Divisors in Associative Algebras over Infinite Fields [Электронный ресурс] / M. Schweitzer, S. Finch. // Режим доступа: arXiv:math.RA/9903182 v1 30 Mar 1999. - P.16.
14. H. E. Bell Noncommutativity and noncentral Zero Divisors. Internat./ H. E. Bell, A. A. Klein // Journal Math. & Math. Sci. —1999. — Vol. 22, No. 1. — P. 67–74.
15. A. Chernitskii Basic Systems of Orthogonal Functions for Space-time Multivectors / A. Chernitskii // Advances in Applied Clifford Algebras. —2005. — Vol. 15, No. 1. — P. 27–54.
16. I.G Bell Multivector Methods [Электронный ресурс] / I.G Bell // Режим доступа: www.iancgbell.clara.net/maths.2007. - P.121.
17. P. Kelly Three-dimensional potential flows from functions of a 3D complex variable / P. Kelly, R. L. Panton // Fluid Dynamics Research . —1990. — Vol. 6. — P. 119–137. — North-Holland.
18. Виноградов И.М. Основы теории чисел / Виноградов И.М. // М. 1952. – 153 с.
19. Розенфельд А.Б. История неевклидовой геометрии. Развитие понятия о геометрическом пространстве / Розенфельд А.Б. // М.: Наука, 1976. – 408с.
20. Study E. Über Systeme von complexen Zahlen / Study E. // Nachrichten von der K.G.D.M. zu Gottingen. —1889.-#9. —S.237-268.
21. Frobenius F.G. Theorie der hyperkomplexen grossen / Frobenius F.G. // Sitzungsber. Akad. Wess. Berlin. – 1903.

22. Clifford W.K. Applications of Grassmann's extensive algebra / Clifford W.K. // Baltimor, 1878. "Mathematical papers", - N. J. 1968. - p. 260-267.
23. Люш В.В. Теория универсальных чисел и приложения ее к решению алгебраических уравнений / Люш В.В. // Труды II Всесоюзного математического съезда. - М.- Изд-во АН СССР, 1936. – Т.2. – С.49-56.
24. И. Л. Кантор. Гиперкомплексные числа / И. Л. Кантор, А. С. Солодовников // М.: Наука, 1973. – 144с.
25. Чернов В.М. Ассоциативно-коммутативные гиперкомплексные алгебры в задачах цифровой обработки многомерных сигналов [Электронный ресурс] / Чернов В.М. // Режим доступа - [www.hypercomplex.ru/ worksforprise.html](http://www.hypercomplex.ru/worksforprise.html). - 2002.
26. Синьков М.В. Непозиционные представления в многомерных числовых системах / Синьков М.В., Губарени Н.М. // Киев: Наукова думка, 1979. –140с.
27. Алгоритмічно-програмний інструментарій аналітичних обчислень над гіперкомплексними числами в системі комп'ютерної математики MAPLE / М.В. Синьков, Я.О. Калиновський, Т.Г. Постнікова, Т.В. Синькова, Ю.Є. Боярінова // Реєстрація, зберігання і обробка даних. — 2005. — Т. 7, № 2. — С. 18–25.
28. Модульні операції над гіперкомплексними числами в системі комп'ютерної математики MAPLE / М.В. Синьков, Я.О. Калиновський, Т.Г. Постнікова, Т.В. Синькова, Ю.Є. Боярінова // Реєстрація, зберігання і обробка даних. — 2005. — Т. 7, № 3. — С. 55–62.
29. О дифференциальных уравнениях, определяющих функции гиперкомплексного переменного / М.В. Синьков, Я.А Калиновський, Ю.Е. Бояринова, А.В. Федоренко // Реєстрація, зберігання і обробка даних. — 2006. — Т. 8, № 3. — С. 20–24.
30. Синьков М.В. Построение алгоритмов решения нестационарных линейных дифференциальных уравнений в гиперкомплексных числовых системах / М.В. Синьков, Я.А Калиновський, Ю.Е. Бояринова, А.В. // Реєстрація, зберігання і обробка даних. — 2006. — Т. 8, № 4. — С. 38–44.

31. Розвиток гіперкомплексного представлення інформації та її застосування / М.В. Синьков, Ю.Є. Боярінова, О.В.Федоренко, Т.Г. Постнікова, Т.В. Синькова // Реєстрація, зберігання і обробка даних. — 2007. — Т. 9, № 4. — С.28—48.
32. Дослідження та використання гіперкомплексних числових систем в задачах динаміки, кінематики та кодування інформації застосування / М.В. Синьков, Ю.Є. Боярінова, О.В.Федоренко, Т.Г. Постнікова, Т.В. Синькова // Пріоритети наукової співпраці ДФФД і БРФФД, Бібліотека Держфонду фундаментальних досліджень. К.: — 2007. — С.21—34.
33. Синьков М. В. Зображення нелінійностей в скінченновимірних гіперкомплексних числових системах / М.В. Синьков, Ю.Є. Боярінова, О.В. Федоренко // Доповіді НАНУ. — 2008. — №8. — С.43—51.
34. Алексейчук А.Н. Модулярная схема разделения секрета над кольцом целых гауссовых чисел / Алексейчук А.Н., Бояринова Ю.Е. // Реєстрація, зберігання і оброб. даних. — 2007. — Т. 9, № 1. — С. 87–99.
35. Разработка структур эффективных цифровых фильтров с помощью гиперкомплексного представления информации / Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Синькова Т.В., Федоренко А.В. // Управління розвитком. — 2006. — № 6. — С. 83–84.
36. Федоренко О.В. Модель цифрового фільтра з гіперкомплексними коефіцієнтами / Федоренко О.В. // Системний аналіз та інформаційні технології: матеріали X Міжн. наук.-техн. конф. – К. : НТУУ „КПІ”, 2008. – С. 413.
37. О.В. Федоренко Цифрові фільтри з низькою параметричною чутливістю / О.В. Федоренко // Реєстрація, зберігання і обробка даних. – 2008. – Т. 10, №2. – С. 87–94.
38. Arora Sanjeev Computational Complexity: A Modern Approach / Arora, Sanjeev; Barak, Boaz (2009) // Cambridge, - 2009. -ISBN 978-0-521-42426-4.
39. Разборов А.А. О сложности вычислений / А. А. Разборов // Математическое просвещение. — МЦНМО, 1999. — № 3. — С. 127-141.

40. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут. — М. : Мир, 1989. — 449 с.
41. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток / Г.Нуссбаумер.-М.-Радио и связь, 1985.-248с.
42. Акушский И.Я. Машинная арифметика в остаточных классах / Акушский И.Я., Юдицкий Д.И. // – М.: Сов. Радио,1968. – 440 с.
43. Asmuth C.A. A modular approach to key safeguarding/ Asmuth C.A., Blum J. // IEEE Transactions on Information Theory, 29, 1983.
44. Blakley G.R. Safeguarding cryptographic keys / Blakley G.R. // In Proceedings AFIPS 1979, Nat. Computer Conf. , 1979
45. Баричев С. Криптография без секретов / Баричев С. // М., - 2002.
46. Hestenes D. Modeling Elastically Coupled Rigid Bodies with Geometric Algebra / Hestenes D., Fasse E. // Preprint. — 2001. — P.13. // Online: <http://modelingnts.la.asu.edu/pdf/ElasticModeling.pdf>
47. Cheng H. H. Dual Polynomials and complex dual Numbers for analysis of spatial Mechanisms / Cheng H. H., Thompson S. // Proceedings of The 1996 ASME Design Engineering Technical Conference and Computers in Engineering Conference. — 1996. — P. 1-12.
48. Cheng H. Programming with Dual Numbers and its Applications in Mechanisms Design / Cheng H. // Engineering with Computers. — 1994. — Vol. 10, No.4. — P.212-229.
49. McCarthy J. Dimensional Synthesis Robots using a Double Quaternion Formulation of the Workspace / McCarthy J, Ahlers S. // Robotics Research: The Ninth International Symposium. — 2000. — P. 3-8.
50. Perez A. Dual Quaternion Synthesis of a Parallel 2-TRP Robot / Perez A., McCarthy J.M. // Proc. of the Workshop on Fundamental Issues and Future Research Directions for Parallel Mechanisms and Manipulators, Quebec City. — 2002.
51. Doik Kim. Analytic Formulation of Reciprocal Screws and Its Application to Nonredundant Robot Manipulators / Doik Kim, Wan Kyun Chung // Journal of Mechanical Design. — 2003. — Vol.125, No. 1. — P.158-164.

52. Ning Ying. Use of Dual euler Angles to describe general spatial Movements of human Joints / Ning Ying, Wangdo Kim // Online: asme.pinetec.com/bio2001/data/pdfs/a0014419.pdf.
53. Бранец В.Н. Применение кватернионов в задачах ориентации твердого тела / Бранец В.Н., Шмыглевский И.П. // М.: Наука, 1973. — 319 с.
54. Калиновский Я.В. Высокорамерные изоморфные гиперкомплексные числовые системы и их использование для повышения эффективности вычислений / Калиновский Я.В., Бояринова Ю.Е. // Инфодрук, 2012.- 183с.
55. Синьков М.В. Конечномерные гиперкомплексные числовые системы. Основы теории. Применения / Синьков М.В., Калиновский Я.А., Бояринова Ю.Е. // К.: Инфодрук, 2010.- 388с.
56. Shoemake K. Animation with quaternions / Shoemake K. // ACM SIGGRAPH course notes 10, Computer animation: 3D Motion, Specification and Control. — 1987.
57. Sangwine S.J. Colour in image processing / Sangwine S.J. // Electronics & Communication Engineering Jour. —2000. — Vol. 12, No. 5, P. 211-219.
58. Mukundan R. Quaternions: From Classical Mechanics to Computer Graphics, and Beyond / Mukundan R. // Proceedings of the 7th Asian Technology Conference in Mathematics. — 2002. — P.97-106.
59. Samareh J. A. Application of Quaternions for Mesh Deformation // 8-th International Conference on Numerical Grid Generation in Computational Field Simulations / Samareh J. A. // Honolulu (Hawaii). — 2002.
60. Бояринова Ю.Е. Разработка алгоритмов восстановления информации в задаче разделения секрета / Бояринова Ю.Е., Одарич Я.В., Трубников П.В. // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 4. — С. 107–112.
61. Бояринова Ю.Е. Реализация алгоритма Евклида для задачи разделения секрета / Бояринова Ю.Е., Одарич Я.В., Трубников П.В. // Реєстрація, зберігання і обробка даних. — 2004. — Т. 6 — № 3. — С. 58–65.
62. Бояринова Ю.Е. Восстановление информации в задаче разделения секрета для гиперкомплексных числовых систем 2-го порядка с помощью алгоритма

Евклида / Бояринова Ю.Е., Одарич Я.В. // Реєстрація, зберігання і обробка даних. — 2004. — Т. 7— № 1. — С. 103–114.

63. Гіперкомплексний RSA-алгоритм / Ланде Д.В., Каліновський Я.О., Бояринова Ю.Є., Хіцко Я.В. // Информационные технологии и безопасность. Оценка состояния: Материалы международной научной конференции ИТБ-2013. - К.: ИПРИ НАН Украины, 2013. - С. 120-124.

64. Kalinovsky, Yakiv O. Applying Hypercomplex Number System to RSA-algorithms / Yakiv O. Kalinovsky, Yuliya E. Boyarinova, Iana V. Khitsko // Advanced CompSystems and Networks: Design and Application. Proceedings of the 6th International Conference, 2013, Ukraine. – 2013. - С.114-115.

65. Toyoshima H. Design of Hypercomplex All-Pass Filters to Realize Complex Transfer Functions / Toyoshima H., Higuchi S. // Proc. Second Int. Conf. Information, Communications and Signal Processing. — 1999Dec. — #2B3.4. — P.1-5.

66. Toyoshima H. Computationally Efficient Implementation of Hypercomplex Digital Filters / Toyoshima H. // IEICE Trans. Fundamentals. — Aug. 2002. — E85-A, 8. — P.1870-1876.

67. Toyoshima H. Computationally Efficient Implementation of Hypercomplex Digital Filters / Toyoshima H. // Proc. Int. Conf. Acoustics, Speech, and Signal processing. — 1998. — Vol. 3. — P.1761-1764. (m5May 1998.)

68. Toyoshima H. Computationally Efficient Bicomplex Multipliers for Digital Signal Processing / Toyoshima H. // IEICE Trans. Inf. & Syst. — Feb. 1998 — E81-D, 2. — P.236-238.

69. Toyoshima H. Complex IIR Digital Filter Composed of Hypercomplex ALL-Pass Filters // Proc. 1995 IEEE Singapore Int. Conf. Signal Processing, Circuits & Systems. — July 1995. — P. 178-183

70. Toyoshima H. Realization of Complex Transfer Functions Using Hypercomplex Digital / Toyoshima H. // Proc. Int. Symp. Information Theory and Its Applications. — Nov1994. — P. 293-298.

71. Изучение специальных видов преобразования базиса в ГЧС второго порядка / Синьков М.В., Калиновский Я.А., Чапор А.А., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 1999. — Т. 1, №2. — С. 39-43.
72. Синьков М.В. Повышение эффективности цифровых фильтров с помощью гиперкомплексного представления информации / Синьков М.В., Калиновский Я.А., Синькова Т.В. // Сборник научных трудов 8-й Международной научной конференции "Теория и техника передачи, приёма и обработки информации" ИИИСТ-2002. — Харьков — 2002. — С. 503-504.
73. Schutte. H.D. Digitalfilter zur Verarbeitung komplexer und hypercomplexer Signale // Dissertation. Paderborn. — 1991. — 100 s.
74. Schutte H.D. Hypercomplex numbers in digital signal processing / Schutte H.D., Wessel J. // In Proc.Int. Conf. On Circuits and Systems. — New Orleans, Louisiana — May 1990. — P. 1557-1560.
75. Калиновский Я.А. Исследование свойств изоморфизма квадриплексных и бикомплексных числовых систем / Калиновский Я.А. // Реєстрація, зберігання і обробка даних. — 2003. — Т. 5, №1. — С. 69-73.
76. Люш В.В. Теория функций триплексного переменного / Люш В.В. // Л.:Изд-во ЛКИ, 1936. —186с.
77. Каратаев Е.А. Сопряжения в гиперкомплексных алгебрах [Электронный ресурс] // Режим доступа - www.karataev.hotmail.ru/conj/index.html - 2002г.
78. Построение сопряжённости в гиперкомплексных числовых системах. Часть 2 / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // On line: <http://www.hypercomplex.ru/sinkov.zip> (2002).
79. Изучение построений сопряжённых элементов в гиперкомплексных числовых системах. Ч.1 / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т. 4, №1. — С. 38-42.
80. Изучение построений сопряжённых элементов в гиперкомплексных числовых системах. Ч.2 / Синьков М. В., Калиновский Я.А., Постникова Т. Г.,

- Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т. 4, №2. — С. 11-15.
81. Построение сопряжённых элементов в гиперкомплексных числовых системах / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // Сб. научн. тр. 8-й Международной научной конференции "Теория и техника передачи, приёма и обработки информации" ИИИСТ-2002, Харьков: 2002. — С. 505-506.
82. Волков Д.М. Аналитические функции в поле гиперкомплексных чисел / Волков Д.М. // Ученые записки ЛГУ, Серия математических наук, 1941. – Вып 12. – №83. – С. 92-113.
83. Маукеев Б. Бикомплексные функции их применения / Маукеев Б., Какимов А., Мейрманова Р. // Рук. депон. в КазНИИНТИЮ. — № 2060. — 06.04.88.
84. Anderson I.M. Introduction to the variational bicomplex / Anderson I.M. // Contemp. Math. — 1992. — No 132. — P. 51-73.
85. Логарифмическая функция от кватерниона / Синьков М.В., Калиновский Я.А., Т.Г. Постникова, Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т.4, №1. — С. 35-37.
86. М.В.Синьков Некоторые линейные и нелинейные операции обобщенных комплексных чисел / М.В.Синьков, Калиновский Я.А., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т.4, №3. — С. 55-61.
87. Fabiano A. An Introduction to the Microlocal Analysis of Hypercomplex Functions [Электронный ресурс] / Fabiano A. — Режим доступа: www.dmi.units.it/~rimut/volumi/28/12fabia.ps.gz - 1996.
88. Casanova G. Parabolic analytic functions // Advances in Applied Clifford Algebras. — 1999. — №2. — P. 221-224.
89. Catoni F. The parabolic analytic Functions and the derivative of real Functions / Catoni F., Cannata R., Nichelatti E. // Advances in Applied Clifford algebras. — 2004. — Vol. 14, No. 2. — P.185-190.
90. Holin H. The Quaternionic Exponential and beyond [Электронный ресурс] Holin H. // Режим доступа - <http://www.bigfoot.com/~Hubert.Holin>.

91. Hubner M. Two-dimensional real Division Algebras revisited / Hubner M., Petersson H.P. // Beiträge zur Algebra und Geometrie. — 2004. — В. 45. — S 29-36.
92. Scheicher K. Elementary Inequalities in Hypercomplex Numbers Anzeiger / Scheicher K., Tichy R. F. , Tomantschger K.W. // 1997.- Abt. II .- No. 134.- S. 3-10.
93. Синьков М.В. Розробка та дослідження алгоритмів побудови зображення обернених функцій від гіперкомплексного змінного / Синьков М.В., Калиновський Я.О., Боярінова Ю.Є. // Реєстрація, зберігання і обробка даних. — 2005. — Т. 7, № 1. — С. 32–42.
94. Построение некоторых функций в гиперкомплексной числовой системе 4-го порядка / Синьков М.В., Калиновский Я.А., Бояринова Ю.Е., Федоренко А.В. // Реєстрація, зберігання і обробка даних. — 2006. — Т. 8 — № 1. — С. 9–16.
95. Nobauer C. The number of isomorphism classes of d.g. near-rings on the generalized quaternion groups / Nobauer C. // Proceedings of the Conference on Near-Rings and Near-Fields, Stellenbosch, South Africa. — 2001. — P. 133 – 137
96. Одарич Я.В. Процедура перечисления гиперкомплексных числовых систем методом линейных преобразований / Одарич Я.В. // Реєстрація, зберігання і обробка даних, том 6, № 2, 2008, стр.107-112.
97. Одарич, Я.В. Перечисление канонических и неканонических гиперкомплексных числовых систем, изоморфных диагональной, и их применение для синтеза цифровых фильтров / Я.В. Одарич // Системный анализ и информационные технологии: материалы X международной научно-технической конференции SAIT 2008, Киев, 20-24 мая 2008 г. / УНК “ИПСА” НТУУ “КПИ”. – К.: УНК “ИПСА” НТУУ “КПИ”, 2008.- С.376.
98. Хицко, Я.В. Исследование классов изоморфизма неканонических гиперкомплексных числовых систем размерности 2 / Я.В. Хицко // Материалы ежегодной итоговой научной конференции ИПРИ НАН Украины, Киев, 2014.
99. Калиновский, Я.А. Исследование классов изоморфизмов неканонических гиперкомплексных числовых систем размерности 2 / Я.А. Калиновский, Я.В.

Хицко, А.С. Туренко // Системный анализ и информационные технологии: материалы XVI международной научно-технической конференции SAIT 2008, Киев, 26-30 мая 2014 г. / УНК “ИПСА” НТУУ “КПИ”. – К.: УНК “ИПСА” НТУУ “КПИ”, 2014.- С.93.

100. Some isomorphic classes for noncanonical hypercomplex number systems of dimension 2 [Электронный ресурс] / Y.O. Kalinovsky, D.V. Lande, Y.E. Boyarinova, I.V. Khitsko // Режим доступа: <http://arxiv.org/abs/1403.2273> - Дата размещения: 07.03.2014.

101. Множинність неканонічних гіперкомплексних числових систем скінченної вимірності / Я.О. Каліновський, Ю.Є. Боярінова, Я.В. Хицко, Н.О. Городько // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. праць. – 2013. - С.35-38.

102. Infinite hypercomplex number system factorization methods [Электронный ресурс] / Y.O. Kalinovsky, D.V. Lande, Y.E. Boyarinova, I.V. Khitsko // Режим доступа: <http://arxiv.org/abs/1401.2844> - Дата размещения: 14.01.2014.

103. Исследование вычислительных операций в гиперкомплексной числовой системе антикватернионов / Я.А. Калиновский, Ю.Е. Бояринова, Я.В. Хицко, А.С. Туренко // Электронное моделирование. – 2014. – Т. 36, №5. - С.49-65.

104. Исследование свойств обобщенных кватернионов и их связей с процедурой удвоения Грассмана-Клиффорда / Я.О. Каліновський, Ю.Є. Боярінова, Я.В. Хицко, А.С. Туренко // Электронное моделирование. – 2015. – Т. 37, №2. – С.17-26.

105. Generalized quaternions and their relations with Grassmann-Clifford procedure of doubling [Электронный ресурс] / Yakiv O Kalinovsky, Yuliya E Boyarinova, Alina S Turenko, Yana V Khitsko // Режим доступа: <http://arxiv.org/abs/1412.8185> - Дата размещения: 28.12.2014.

106. Изучение построений сопряжённых элементов в гиперкомплексных числовых системах. Ч.1 / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т. 4, №1. — С. 38-42.

107. Изучение построений сопряжённых элементов в гиперкомплексных числовых системах. Ч.2 / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т. 4, №2. — С. 11-15.
108. Калиновский Я.А. Построение норм и сопряженных чисел в изоморфных гиперкомплексных числовых системах / Калиновский Я.А. // Реєстрація, зберігання і обробка даних. — 2011. — Т. 13, №3. — С. 17-29.
109. Одарич, Я.В. Вычисления в неканонических гиперкомплексных числовых системах / Я.В. Одарич, Е.Ю. Наливайчук, Н.В. Наливайчук // Радіоелектронні і комп'ютерні системи. – Вип. 5. - 2010. – С.75-78.
110. Синьков М.В. Повышение эффективности цифровых фильтров с помощью гиперкомплексного представления информации / Синьков М.В., Калиновский Я.А., Синькова Т.В. // Сборник научных трудов 8-й Международной научной конференции "Теория и техника передачи, приёма и обработки информации" ИИИСТ-2002. — Харьков — 2002. — С. 503-504.
111. Бизин, А. Т. Введение в цифровую обработку сигналов / А.Т. Бизин — Новосибирск, 1998. — 66 с.
112. Калиновский, Я.А. Применение неканонических гиперкомплексных числовых систем для оптимизации суммарной параметрической чувствительности реверсивных цифровых фильтров / Я.А. Калиновский, Ю.Е. Бояринова, Я.В. Хицко // Реєстрація, зберігання і обробка даних. – Т. 16 № 4. – 2014. - С.3-11.
113. Reversible Digital Filters Total Parametric Sensitivity Optimization using Non-canonical Hypercomplex Number Systems [Електронний ресурс] / Yakiv O. Kalinovsky, Yuliya E. Boyarinova, Iana V. Khitsko // Режим доступу: <http://arxiv.org/abs/1506.01701> - Дата розміщення: 25.01.2015.
114. Каліновський Я.О. Синтез реверсивних цифрових фільтрів із застосуванням неканонічних гіперкомплексних числових систем та оптимізація

їх параметричної чутливості / Каліновський Я.О., Хицко Я.В. // Матеріали
ежегодной итоговой научной конференции ИПРИ НАН Украины, Киев, 2015.

115. Калиновский Я.А. Оптимизация суммарной параметрической чувствительности реверсивных цифровых фильтров с коэффициентами в неканонических гиперкомплексных числовых системах. / Я.А. Калиновский, Ю.Е. Бояринова, Я.В. Хицко // Электронное моделирование. – 2015. – Т. 37, №5. - С.117-126.

Приложение А. Справка про использование результатов диссертационной работы

THE STATE CONCERN
«UKROBORONPROM»
DP SCIENTIFIC INDUSTRIAL COMPLEX
“PROGRES”

29, Nosivsky Shlyakh St., Nizhin
Chernihiv Region. 16610, Ukraine
For telegram “ALMAZ”
Teletype 192847
Fax (38 - 04631) 5 - 47 - 46
Tel (38 - 04631) 5 - 47 - 78
e-mail: progress@ukr.net



ДЕРЖАВНИЙ КОНЦЕРН
«УКРОБОРОНПРОМ»
ДП НАУКОВО-ВИРОБНИЧИЙ КОМПЛЕКС
«ПРОГРЕС»

Україна. 16610, м. Ніжин Чернігівської обл.,
вул. Носівський шлях, 29
Для телеграм “АЛМАЗ”
Телетайп 192847
Факс (38 - 04631) 5 - 47 - 46
Тел (38 - 04631) 3-17 - 36
e-mail: progress@ukr.net

10.06.2015 р. № 232/288

ДОВІДКА

Ця Довідка видана Хіцко Яні Володимирівні в тому, що результати її досліджень по застосуванню неканонічних гіперкомплексних числових систем для оптимізації сумарної параметричної чутливості реверсивних цифрових фільтрів, що виконані в Інституті проблем реєстрації інформації НАН України, використані :

1. В алгоритмі роботи цифрових фільтрів програмного забезпечення координато вимірювальної машини CONTURA G2 в режимі сканування внутрішніх поверхонь деталей типу «циліндричний отвір»;
2. В розділі «Рекомендації» проекту Державного Стандарту України ДСТУ ISO 10360-2:2014 (проект) Технічні вимоги до геометрії виробів (GPS). Приймальні та контрольні випробування координатно-вимірювальних машин.

ГОЛОВНИЙ ІНЖЕНЕР ДП НВК «ПРОГРЕС»



[Handwritten signature] В.М.ШИМКО

Приложение Б. Структура программно-аналитического инструментария в пакете MAPLE



Приложение В. Листинги кода программно-аналитического инструментария в пакете MAPLE

1. Операция сложения

```
> # Операция сложения двух гиперкомплексных чисел
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> Addition:=proc(A, B, n, Variables) local i, Res;
>   Res:=0;
>   for i from 1 to n do
>Res:= Res + (coeff(A, Variables[i])+coeff(B, Variables[i]))*Variables[i];
>   od;
> return (Res);
> end proc;
```

Таким образом, мы можем получить сумму двух заданных чисел как в общем виде, так и для конкретных коэффициентов. Например, для систем третьей размерности:

```
> E_seq:={seq(E[i], i=0..2)};
> A:=a[0]*E[0]+a[1]*E[1]-a[2]*E[2];
> B:=b[0]*E[0]-b[1]*E[1]+b[2]*E[2];
> C:=Addition(A,B,3,E_seq);
A := a0E0 + a1E1 + a2E2
B := b0E0 + b1E1 + b2E2
C := (a0 + b0)E0 + (a1 + b1)E1 + (a2 + b2)E2
```

2. Операция вычитания

```
> # Операция вычитания двух гиперкомплексных чисел
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> Substraction:=proc(A, B, n, Variables) local i, Res;
>   Res:=0;
>   for i from 1 to n do
>Res:=Res+(coeff(A, Variables[i])-coeff(B, Variables[i]))*Variables[i];
>   od;
> return (Res);
> end proc;
```

Получаем разницу в общем виде для систем размерности 3:

```
> E_seq:={seq(E[i], i=0..2)};
> A:=a[0]*E[0]+a[1]*E[1]+a[2]*E[2];
> B:=b[0]*E[0]+b[1]*E[1]+b[2]*E[2];
> C:=Substraction(A,B,3,E_seq);
A := a0E0 + a1E1 + a2E2
B := b0E0 + b1E1 + b2E2
C := (a0 - b0)E0 + (a1 - b1)E1 + (a2 - b2)E2
```

3. Операция умножения

```
> # Операция умножения двух гиперкомплексных чисел
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной систем
```

```

> Mult:=proc(A,B,n, Variables, Mult_table) local i,j,k, Res;
>   Res:=0;
>   for i from 1 to n do
>     for j from 1 to n do
>       for k from 1 to n do
>         Res:= Res + coeff(A,Variables[i])*coeff(B,Variables[j])*
coeff(Mult_table[i,j], Variables[k])*Variables[k];
>       od;
>     od;
>   od;
> return (Res);
> end proc;

```

Для примера, используем удвоение системы W в качестве гиперкомплексной числовой системы $W^{(2)}(W,W,4)$:

$$Mult_TableWW := \begin{bmatrix} E_0 & E_1 & E_2 & E_3 \\ E_1 & E_0 & E_3 & E_2 \\ E_2 & E_3 & E_0 & E_1 \\ E_3 & E_2 & E_1 & E_0 \end{bmatrix}$$

```

> E_seq:={seq(E[i], i=0..3)};
> A:=a[0]*E[0]+a[1]*E[1]+a[2]*E[2]+a[3]*E[3];
> B:=b[0]*E[0]+b[1]*E[1]+b[2]*E[2]+b[3]*E[3];
> C:=Mult(A,B,4,E_seq, Mult_TableWW);

```

$$A := a_0 E_0 + a_1 E_1 + a_2 E_2 + a_3 E_3$$

$$B := b_0 E_0 + b_1 E_1 + b_2 E_2 + b_3 E_3$$

$$C := a_0 b_0 E_0 + a_0 b_1 E_1 + a_0 b_2 E_2 + a_0 b_3 E_3 + a_1 b_0 E_1 + a_1 b_1 E_0 + a_1 b_2 E_3 + a_1 b_3 E_2 + a_2 b_0 E_2 + a_2 b_1 E_3 + a_2 b_2 E_0 + a_2 b_3 E_1 + a_3 b_0 E_3 + a_3 b_1 E_2 + a_3 b_2 E_1 + a_3 b_3 E_0$$

4. Единичный элемент

```

> # Поиск единичного элемента гиперкомплексной числовой системы
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной систем
> One_E:=proc(n, Variables, Mult_table) local i,j,k, M, OneEquation, X_sol,
results, Res;
# строим систему уравнений, основываясь на коэффициентах при базисных элементах
> for i from 1 to n do
>   OneEquation[i]:=-a[i-1];
>   for j from 1 to n do
>     for k from 1 to n do
>       OneEquation[i]:=OneEquation[i]+a[j-1]*x[k-1]*coeff(Mult_table[j,k],
Variables[i]);
>     od;
>   od;
> od;
> results:={seq(x[i], i=0..n-1)};
> # получаем решение системы
> X_sol:= {solve(convert(OneEquation,set), results )};
> # если решений нет - возвращаем нулевой единичный элемент
> if (nops(X_sol)=0) then
>   return 0;
> end if;
> Res:=0;
> # форматируем полученное решение в гиперкомплексное число
> for i from 1 to n do

```



```

> Res:=Res + subs(X_sol[1],x[i-1])*Variables[i];
> od;
> return Res;
> end proc;

```

Объявим гиперкомплексную систему размерности 3 через таблицу умножения и найдем ее единичный элемент.

```

> E_seq:={seq(E[i],i=0..2)};
> Mult_Table3E:=array(1..3, 1..3, [[-2*E[0]-E[1],-E[1],-2*E[2]],[-E[1], E[1],0],
[-2*E[2],0,2*E[0]+E[1]]]);
> One3E:=One_E(3, E_seq, Mult_Table3E);

```

$$Mult_Table3E := \begin{bmatrix} -2E_0 - E_1 & -E_1 & -2E_2 \\ -E_1 & E_1 & 0 \\ -2E_2 & 0 & 2E_0 + E_1 \end{bmatrix}$$

$$One3E := -\frac{1}{2}E_0 + \frac{1}{2}E_1$$

5. Определение нормы гиперкомплексного числа

```

> # Определение нормы гиперкомплексного числа
> # A - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной системы
> Norm_HNS:=proc(A, n, Variables, Mult_table) local i,j,k, Norm_matrix;
> Norm_matrix:=Matrix(n,n); # формируем матрицу для определения нормы
> for i from 1 to n do
>   for j from 1 to n do
>     Norm_matrix[i,j]:=0;
>     for k from 1 to n do
>
>       Norm_matrix[i,j]:=Norm_matrix[i,j]+coeff(A,
Variables[k])*coeff(Mult_table[i,j], Variables[k]);
>     od;
>   od;
> od;
> return Determinant(Norm_matrix);
> end proc;

```

Найдем норму числа в системе триплексных чисел в общем виде.

```

> E_seq:={seq(E[i], i=0..2)};
> MultTableTriplex:=array(1..3, 1..3, [[E[0],E[1],E[2]], [E[1],0.5*(-E[0]+E[2]),-
E[1]], [E[2],-E[1],E[0]]]);
> A:=a[0]*E[0]+a[1]*E[1]+a[2]*E[2];
> N := Norm_HNS(A,3,E_seq, MultTableTriplex);

```

$$MultTableTriplex := \begin{bmatrix} E_0 & E_1 & E_2 \\ E_1 & -0.5E_0 + 0.5E_2 & -E_1 \\ E_2 & -E_1 & E_0 \end{bmatrix}$$

$$A := a_0 E_0 + a_1 E_1 + a_2 E_2$$

$$N := -0.5a_0^3 + 0.5a_0^2a_2 - 2a_0a_1^2 - 2a_1^2a_2 + 0.5a_0a_2^2 - 0.5a_2^3$$

6. Делитель нуля

```

> # Возвращает true, если заданное число является делителем нуля
> # A - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной системы
> Nullsys_HNS:=proc(A, n, Variables, Mult_table);
> # если норма числа равна нулю, возвращаем true

```

```

>   if (Norm_HNS(A,n,Variables,Mult_table)=0) then
>     return true;
>   else
>     return false;
>   end if;
> end proc;

```

Выполним проверку для некоторых чисел из системы двойных чисел. Норма системы двойных чисел выглядит таким образом: $N(A) = a_0^2 - a_1^2$, где $A = a_0 * E_0 - a_1 * E_1$. Тогда для делителей нуля справедливо $a_0^2 = a_1^2$. Проверим процедуру Nullsys_HNS для числа, которое удовлетворяет данному условию:

```

> E_seq:={seq(E[i], i=0..1)};
> Mult_TableW:= array(1..2, 1..2, [[E[0],E[1]], [E[1],E[0]]]);
> A:=a[0]*E[0]-a[0]*E[1];
> Nulls:=Nullsys_HNS(A,2,E_seq,Mult_TableW);

```

$$Mult_TableW := \begin{bmatrix} E_0 & E_1 \\ E_1 & E_0 \end{bmatrix}$$

$$A := a_0 E_0 - a_0 E_1$$

$$Nulls := true$$

Проверим процедуру для числа с вещественными коэффициентами:

```

> A:=2*E[0]-E[1];
> Nulls:=Nullsys_HNS(A,2,E_seq,Mult_TableW);
      A := 2 E_0 - E_1
      Nulls := false

```

7. Произведение сопряженных

```

> # Поиск произведения сопряженных гиперкомплексному числу
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной системы
> # normA - 0 или уже вычисленная норма числа A
> Conjugate_HNS:=proc(A, n, Variables, Mult_table, normA) local i,j,k, OneEl,
N_A, ConEquation, X_sol, results, Res;
> # сначала находим единичный элемент системы
>   OneEl:=One_E(n, Variables, Mult_table);
> # находим норму числа A
>   if (normA = 0) then
>     N_A:=Norm_HNS(A, n, Variables, Mult_table);
>   else
>     N_A:=normA;
>   end if;
> # составляем систему уравнений
> #
> # A* A = N(A)*X
>   for i from 1 to n do
>     ConEquation[i]:=-N_A*coeff(OneEl,Variables[i]);
>     for j from 1 to n do
>       for k from 1 to n do
>         ConEquation[i]:=ConEquation[i]+coeff(A,Variables[j])*x[k-
1]*coeff(Mult_table[j,k], Variables[i]);
>       od;
>     od;
>   od;
> results:={seq(x[i], i=0..n-1)};
> X_sol:= {solve(convert(ConEquation,set),results )};
> if (nops(X_sol)=0) then
>   return 0;

```

```

> end if;
> Res:=0;
> # преобразуем полученные результаты в вид гиперкомплексного числа
> for i from 1 to n do
>   Res:=Res + subs(X_sol[1],x[i-1])*Variables[i];
> od;
> return Res;
> end proc;

```

Найдем произведение сопряженных в гиперкомплексной системе $W^{(2)}(W,W,4)$ (удвоение системы двойных чисел на основе процедуры Грассмана – Клиффорда).

```

>Mult_TableWW:= array(1..4, 1..4, [[E[0],E[1],E[2],E[3]],
[E[1],E[0],E[3],E[2]], [E[2],E[3],E[0],E[1]], [E[3],E[2],E[1],E[0]]]);
> A:=b[0]*E[0]+b[1]*E[1]+b[2]*E[2]+b[3]*E[3];
> E_seq:={seq(E[i], i=0..3)};
> A_conj:=Conjugate_HNS(A,4,E_seq,Mult_TableWW, 0);

```

$$Mult_TableWW := \begin{bmatrix} E_0 & E_1 & E_2 & E_3 \\ E_1 & E_0 & E_3 & E_2 \\ E_2 & E_3 & E_0 & E_1 \\ E_3 & E_2 & E_1 & E_0 \end{bmatrix}$$

$$A := b_0 E_0 + b_1 E_1 + b_2 E_2 + b_3 E_3$$

$$b_0^4 - 2b_0^2 b_1^2 + 8b_0 b_3 b_1 b_2 - 2b_3^2 b_0^2 - 2b_0^2 b_2^2 + b_1^4 - 2b_3^2 b_1^2 - 2b_1^2 b_2^2 + b_2^4 - 2b_2^2 b_3^2 + b_3^4$$

$$A_conj := (b_0^3 - b_0 b_1^2 + 2b_3 b_1 b_2 - b_3^2 b_0 - b_0 b_2^2) E_0 + (b_1^3 - b_3^2 b_1 - b_1 b_0^2 - b_1 b_2^2 + 2b_3 b_0 b_2) E_1 + (2b_1 b_3 b_0 - b_1^2 b_2 - b_0^2 b_2 + b_2^3 - b_2 b_3^2) E_2 + (-b_3 b_1^2 + 2b_1 b_0 b_2 + b_3^3 - b_3 b_0^2 - b_3 b_2^2) E_3$$

Найдем произведение сопряженных для системы триплексных чисел.

```

> MultTableTriplex:=array(1..3, 1..3, [[E[0],E[1],E[2]], [E[1],0.5*(-E[0]+E[2]),-E[1]], [E[2],-E[1],E[0]]]);
> A:=b[0]*E[0]+b[1]*E[1]+b[2]*E[2];
> E_seq:={seq(E[i], i=0..2)};
> N:=-0.5*(b[0]^3+b[0]^2*b[2]+b[0]*b[2]^2-b[2]^3)-2*(b[0]*b[1]^2+b[1]^2*b[2]);
> A_conj:=Conjugate_HNS(A,3,E_seq,MultTableTriplex, N);

```

$$MultTableTriplex := \begin{bmatrix} E_0 & E_1 & E_2 \\ E_1 & -0.5E_0 + 0.5E_2 & -E_1 \\ E_2 & -E_1 & E_0 \end{bmatrix}$$

$$A := b_0 E_0 + b_1 E_1 + b_2 E_2$$

$$N := -0.5b_0^3 - 0.5b_0^2 b_2 - 0.5b_0 b_2^2 + 0.5b_2^3 - 2b_0 b_1^2 - 2b_1^2 b_2$$

$$\begin{aligned}
A_{conj} := & -\left(0.2500000000 \left(b_0^3 + b_0^2 b_2 + b_0 b_2^2 + 4. b_0 b_1^2 - 1. b_2^3 + 4. \right. \right. \\
& \left. \left. b_1^2 b_2\right) \left(2. b_0^2 - 2. b_0 b_2 + b_1^2\right) E_0\right) / \left(b_1^2 b_2 + b_0 b_1^2 - 1. b_0^2 b_2 + b_2^3 \right. \\
& \left. + b_0^3 - 1. b_0 b_2^2\right) \\
& + \frac{1}{b_0^2 - 2. b_0 b_2 + b_1^2 + b_2^2} \left(0.5000000000 \left(b_0^3 + b_0^2 b_2 + b_0 b_2^2 \right. \right. \\
& \left. \left. + 4. b_0 b_1^2 - 1. b_2^3 + 4. b_1^2 b_2\right) b_1 E_1\right) + \left(0.2500000000 \left(-1. \right. \right. \\
& \left. \left. b_1^2 b_0^3 + 7. b_1^2 b_0^2 b_2 - 1. b_1^2 b_0 b_2^2 - 7. b_1^2 b_2^3 - 4. b_1^4 b_0 - 4. b_1^4 b_2 \right. \right. \\
& \left. \left. + 2. b_2^5 + 2. b_0^4 b_2 - 4. b_0 b_2^4\right) E_2\right) / \left(b_1^2 b_2 + b_0 b_1^2 - 1. b_0^2 b_2 + b_2^3 \right. \\
& \left. + b_0^3 - 1. b_0 b_2^2\right)
\end{aligned}$$

8. Деление

```

> # Деление одного гиперкомплексного числа на другое число
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # Mult_table - таблица умножения заданной системы
> Devision:=proc(A, B, n, Variables, Mult_table) local ConjB,Dev, NormB;
>   NormB:=Norm_HNS(B, n, Variables, Mult_table);
>   ConjB:=Conjugate_HNS(B, n, Variables, Mult_table, NormB);
>   Dev:=Mult(A, ConjB, n, Variables, Mult_table)/NormB;
>   return Dev;
> end proc;

```

Вычислим деление чисел в системе двойных чисел в общем виде:

```

> E_seq:={seq(E[i], i=0..1)};
> Mult_TableW:= array(1..2, 1..2, [[E[0],E[1]],[E[1],E[0]]]);
> A:=a[0]*E[0]+a[1]*E[1]; B:=b[0]*E[0]+b[1]*E[1];
> Dev:=Devison(A, B, 2,E_seq,Mult_TableW);

```

$$\begin{aligned}
Mult_TableW &:= \begin{bmatrix} E_0 & E_1 \\ E_1 & E_0 \end{bmatrix} \\
A &:= a_0 E_0 + a_1 E_1 \\
B &:= b_0 E_0 + b_1 E_1 \\
Dev &:= \frac{a_0 b_0 E_0 - a_0 b_1 E_1 + a_1 b_0 E_1 - a_1 b_1 E_0}{b_0^2 - b_1^2}
\end{aligned}$$

Найдем частное от деления двух чисел в системе бикомплексных чисел.

```

> E_seq:={seq(E[i], i=0..3)};
> Mult_TableCC:= array(1..4, 1..4, [[E[0],E[1],0,0],[E[1],-E[0],0,0],[0,0,E[2],E[3]],[0,0,E[3],-E[2]]]);
> A:=2*E[0]+E[1]-E[2]+3*E[3]; B:=E[0]+E[1]+2*E[2]-E[3];
> Dev:=Devison(A, B, 4,E_seq,Mult_TableCC);

```

$$\begin{aligned}
Mult_TableCC &:= \begin{bmatrix} E_0 & E_1 & 0 & 0 \\ E_1 & -E_0 & 0 & 0 \\ 0 & 0 & E_2 & E_3 \\ 0 & 0 & E_3 & -E_2 \end{bmatrix} \\
A &:= 2 E_0 + E_1 - E_2 + 3 E_3 \\
B &:= E_0 + E_1 + 2 E_2 - E_3
\end{aligned}$$

$$Dev := \frac{3}{2} E_0 - \frac{1}{2} E_1 - E_2 + E_3$$

8. Переход из одной системы в изоморфную ей

```
> # Конвертация числа из одной системы в другую с помощью заданных правил
изоморфного перехода
> # A - гиперкомплексное число
> # n - размерность системы
> # Variables - базисные элементы новой системы
> # ConvertRules - правила изоморфного перехода
> ConvertSystem:=proc(A, n, Variables, ConvertRules) local i, Res;
>   Res:=0;
>   for i from 1 to n do
>     Res:=Res + coeff(A, Variables[i])*ConvertRules[i];
>   od;
> return expand(Res);
> end proc;
```

Переведем число из двойной системы W в систему $R \oplus R$ и обратно.

```
> ConvertRulesE:=[R[0]+R[1], R[0]-R[1]];
> ConvertRulesR:=[0.5*(E[0]+E[1]), 0.5*(E[0]-E[1])];
> R_seq:={R[0], R[1]};
> E_seq:={E[0], E[1]};
> A:=5*E[0]-E[1];
> A_r:=ConvertSystem(A, 2, E_seq, ConvertRulesE);
> A_e:=ConvertSystem(A_r, 2, R_seq, ConvertRulesR);
      ConvertRulesE := [R0 + R1, R0 - R1]
      ConvertRulesR := [0.5 E0 + 0.5 E1, 0.5 E0 - 0.5 E1]
      A := 5 E0 - E1
      A_r := 4 R0 + 6 R1
      A_e := 5.0 E0 - 1.0 E1
```

9. Вычисление вычета в неканонических ГЧС

```
> # Операция вычисления вычета неканонического гиперкомплексного числа
> # A - гиперкомплексное число
> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # mult_table - таблица умножения системы
> Remainder:=proc(A,B,n,Variables, mult_table) local i,j,k,Res,rem_local,
Conj_b, Mult_a_conj_b, N_b;
>   Res:=0; rem_local:=0;
>   N_b:=round(Norm_HNS(B,n,Variables,mult_table));
>   Conj_b:=Conjugate_HNS(B, n, Variables, mult_table, N_b);
>   Mult_a_conj_b:=Mult(Conj_b, A, n, Variables, mult_table);
>   for i from 1 to n do
>     rem_local:= rem_local +
mods(coeff(Mult_a_conj_b,Variables[i]),N_b)*Variables[i];
>   od;
>   rem_local:=Mult(rem_local,B,n,Variables,mult_table);
>   for i from 1 to n do Res:=Res + (coeff(rem_local,
Variables[i])/N_b)*Variables[i]; od;
>   return(Res);
> end proc;
```

10. Алгоритм Евклида для неканонических ГЧС

```
> # Алгоритм Евклида для неканонических гиперкомплексных чисел
> # A - гиперкомплексное число
```

```

> # B - гиперкомплексное число
> # n - размерность системы
> # Variables - набор базисных элементов
> # mult_table - таблица умножения системы
> Euklid:=proc(A , B, n, Variables, mult_table) local x0, x1, y0, y1, q, r0, r1,
r2, x2, y2, i, Check, AX_, BY_;
> x0:=One_E(n, Variables, mult_table); y1:=x0;
> x1:=0; y0:=0; r0:=A; r1:=B;
> while (IsNull(r1, n) <> true) do
>   if (Nullsys_HNS(r1, n, Variables, mult_table) = true) then return 0;
end if;
>   r2:=Remainder( r0, r1, n, Variables, mult_table);
>   q:=Substraction( r0, r2, n, Variables, mult_table);
>   q:=Devison( q, r1, n, Variables, mult_table );
>
>   x2:=Mult(q, x1, n, Variables, mult_table);
>   x2:=Substraction(x0, x2, n, Variables, mult_table );
>
>   y2:=Mult(q, y1, n, Variables, mult_table);
>   y2:=Substraction(y0, y2, n, Variables, mult_table );
>
>   r0:=r1; x0:=x1; y0:=y1;
>   r1:=r2; x1:=x2; y1:=y2;
> od;
> x0:=Devison(x0, r0, n, Variables, mult_table);
> y0:=Devison(y0, r0, n, Variables, mult_table);
>
> return x0;
> end proc:

```

11. Процедура перечисления неканонических ГЧС изоморфных заданной

```

> # Процедура генерации системы уравнений для изоморфного перехода
> # index - индекс ячейки в таблице умножения
> # n - размерность системы
> # N - количество перебираемых ячеек
> Generate_matrix := proc(index, n, N) local i,j,t; global aSteps,InvertedStep,
Border, aEquation, aUnit;
> if (index < N) then
>   i:=floor( index/n); j:=index mod n;
>   if (j=0) then aEquation[i]:=-E[i+1]; end if;
>   if (i=0) then
>     aEquation[i]:=aEquation[i]+aUnit;
>     Generate_matrix(index+n,n,N);
>   else
>     for t from Border*InvertedStep by -1 to -Border*InvertedStep do
>       aSteps[i,j]:=t/InvertedStep;
>       aEquation[i]:=aEquation[i] + (t/InvertedStep)*r[j+1];
>       if (index = N-1) then
>         Solve_system(n,N);
>       else
>         Generate_matrix(index+1,n,N);
>       end if;
>       aEquation[i]:=aEquation[i] - (t/InvertedStep)*r[j+1];
>     od;
>   end if;
> end if;
> end proc:

> # Процедура решения системы уравнений изоморфного перехода
> Solve_system:=proc() local flag; global a,N_sol, results, resultsR, aSteps,
aEE, aRR, aEquation, Counter, aSystems, aGivenSystem;
>

```

```

> if (Det(aSteps)<>0) then
>
>   a := {solve(convert(aEquation,set),resultsR )};
>   N_sol:=nops(a);
>
>   if (N_sol = 0) then return (0): end if;
>   b:={solve(a[1], results)}; #print(b[1]); print(a[1]);
>   for i from 0 while i<n do
>     for j from 0 while j<n do
>       aEE[i,j]:=expand(subs(b[1], E[i+1])* subs(b[1],E[j+1]));
>       for t from 0 to N-1 do
>         i_t:=floor(t/n); j_t:=t mod n;
>         if(i_t=j_t) then
aEE[i,j]:=expand(algsubs(r[i_t+1]^2=aGivenSystem[t+1], aEE[i,j]));
>         else
aEE[i,j]:=expand(algsubs(r[i_t+1]*r[j_t+1]=aGivenSystem[t+1], aEE[i,j])); end
if;
>         od:
>         aRR[i,j]:= algsubs(r[1]=subs(a[1], r[1] ), aEE[i,j]) ;
>         for t from 2 to N do
>           aRR[i,j]:= algsubs(r[t]=subs(a[1], r[t] ) , aRR[i,j] );
>         od:
>       od;
>     od;
>   bCopy:= true;
>   for k from 0 while (k<Counter) and (bCopy=true) do
>     if(Are_Equal(aSystems,aRR, k, n) = true) then bCopy:=false; end if;
>   od;
>   if (bCopy=true) then
>     bCopy:=Linear_Independance(aRR,n);
>   end if;
>   if (bCopy=true) then
>     Copy_Matrix(aSystems,aRR,Counter,n);
>     Counter:=Counter+1;
>     print("Counter=",Counter);
>     print ("aRR=",aRR);
>   end if;
> end if;
> end proc:

```

Приложение Г. Неканонические ГЧС, изоморфные комплексным числам

E_1	E_2
E_2	$-32E_1 - 8E_2$

E_1	E_2
E_2	$-13E_1 - 4E_2$

E_1	E_2
E_2	$-25E_1 - 8E_2$

E_1	E_2
E_2	$-8E_1 - 4E_2$

E_1	E_2
E_2	$-17E_1 - 8E_2$

E_1	E_2
E_2	$-5E_1 - 4E_2$

E_1	E_2
E_2	$-25E_1 - 6E_2$

E_1	E_2
E_2	$-17E_1 - 2E_2$

E_1	E_2
E_2	$-18E_1 - 6E_2$

E_1	E_2
E_2	$-10E_1 - 2E_2$

E_1	E_2
E_2	$-13E_1 - 6E_2$

E_1	E_2
E_2	$-5E_1 - 2E_2$

E_1	E_2
E_2	$-10E_1 - 6E_2$

E_1	E_2
E_2	$-2E_1 - 2E_2$

E_1	E_2
E_2	$-20E_1 - 4E_2$

E_1	E_2
E_2	$-16E_1$

E_1	E_2
E_2	$-9E_1$

E_1	E_2
E_2	$-5E_1 + 4E_2$

E_1	E_2
E_2	$-4E_2$

E_1	E_2
E_2	$-25E_1 + 6E_2$

E_1	E_2
E_2	$-17E_1 + 2E_2$

E_1	E_2
E_2	$-13E_1 + 6E_2$

E_1	E_2
E_2	$-10E_1 + 2E_2$

E_1	E_2
E_2	$-18E_1 + 6E_2$

E_1	E_2
E_2	$-5E_1 + 2E_2$

E_1	E_2
E_2	$-10E_1 + 6E_2$

E_1	E_2
E_2	$-2E_1 + 2E_2$

E_1	E_2
E_2	$-32E_1 + 8E_2$

E_1	E_2
E_2	$-20E_1 + 4E_2$

E_1	E_2
E_2	$-25E_1 + 8E_2$

E_1	E_2
E_2	$-13E_1 + 4E_2$

E_1	E_2
E_2	$-17E_1 + 8E_2$

E_1	E_2
E_2	$-8E_1 + 4E_2$