ОТЗЫВ

официального оппонента доктора физико-математических наук Винокурова Сергея Федоровича на диссертацию **Кукарцева Анатолия Михайловича** на тему **«Эффективные алгоритмы анализа джевонс-эквивалентности данных»**, представленную на соискание учёной степени **кандидата физико-математических наук** по специальности **05.13.17 – Теоретические основы информатики**

Актуальность темы диссертационной работы

Соискателем рассматривается представление информации дискретными функциями с последующим заданием над ними отношений эквивалентности. Актуальность выбранного направления не вызывает сомнений и отражает современные подходы к описанию данных и заданию методов обработки над ними. Соискатель исследует задачу определения джевонс-эквивалентности данных. Выбранная область исследования включает в себя действие элементов группы Джевонса над булевыми функциями. Действие реализуется посредством перестановки и (или) отрицания аргументов булевой функции. Такое действие интранзитивно и разбивает всё множество булевых функций на непересекающиеся классы (орбиты). Задачи определения принадлежности двух функций одной орбите и вычисление действующих элементов группы допускают тривиальные решения (перебор всех элементов группы), но при этом являются сложнорешаемыми в силу экспоненциального порядка группы.

Интерес к группе Джевонса связан также и с построением расширений этой группы, активно исследуемых в отечественных и западных научных школах. Оказалось, что расширение до аффинной эквивалентности сохраняет количество единиц в векторе, но не сохраняет количество слагаемых в полиноме, а расширение до операторной эквивалентности сохраняет количество слагаемых в полиноме, но не сохраняет количество единиц в векторе. И только преобразования из группы Джевонса сохраняют и количество единиц в векторном представлении булевой функции и количество слагаемых в ее полиномиальном представлении, что существенно для различных приложений.

Выбранные соискателем задачи сформулированы первоначально в области дискретной математики как задачи классификации функций, затем рассмотрены их приложения в актуальных направлениях обработки информации и криптографии.

Оценка диссертационной работы

Текст диссертации представлен на 119 страницах. Он включает в себя введение, четыре главы, заключение, список литературы, список сокращений и условных обозначений, а также четыре приложения.

Во введении обоснованна актуальность, поставлены цель и задачи исследования, сформулированы новые полученные результаты, а также приведены сведения об апробации и публикации результатов работы.

В первой главе рассматривается проблема выбора представления группы Джевонса для действия над булевыми функциями. Предложенный соискателем метод выбора представления группы Джевонса сводится к выбору гомоморфизма полупрямого внешнего произведения.

Соискатель рассматривает термальные и векторные представления булевых функций. Действие группы Джевонса определяется над термальными представлениями, далее над векторными представлениями индуцируется действие подгруппы симметрической группы эквивалентное действию группы Джевонса. Полученная действующая подгруппа в действительности является изоморфным образом группы Джевонса и представляется внутренним полупрямым произведением. Из гомоморфизма этого внутреннего произведения соискатель строит гомоморфизм для группы Джевонса. В этой же главе вводится единая в рамках всего изложения система обозначений.

Вторая глава преимущественно описывает действия полученных представлений группы Джевонса над бинарными векторами и булевыми функциями. Описание содержит необходимые определения и доказательства. Из текста второй главы фактически доказывается необходимость именно двух представлений группы Джевонса типа А и типа Б. Первая часть второй главы является изложением правил по которым производятся действия группы Джевонса над бинарными векторами и булевыми функциями. Вторая часть главы содержит качественно новые частотные свойства рассматриваемых действий. Приводятся доказательства частотных (энтропийных) свойств действий группы Джевонса над функциями.

Третья глава является ядром диссертационной работы и содержит три части. В первой описывается и доказывается факт существования монотонного представления подстановки и канонического представления элемента группы Джевонса. Во второй части приводится основной алгоритм определения джевонс-эквивалентности данных. В третьей части предлагается серия алгоритмов, которые являются дополнением к основному и предназначены для параллельного вычисления действия элементов группы Джевонса над функциями. Все алгоритмы имеют вычислительные обоснования.

Четвёртая глава описывает различные подходы к оценке сложности предложенного основного алгоритма анализа джевонс-эквивалентности данных. Она включает в себя не только теоретические оценки, но и проведённые компьютерные эксперименты над большим количеством фрагментов данных различного размера. В главе также приводится статистика мощностей и числа орбит относительно группы Джевонса.

В заключении приведены выводы по проделанной работе и сформулированы дальнейшие пути развития рассматриваемой предметной области.

Список условных обозначений и сокращений содержит все встречаемые в тексте работы сокращения.

Список литературы включает 72 позиции. Соискателем использованы наиболее свежие работы, затрагивающие группу Джевонса и её действия над булевыми функциями (крайние даты публикации – 2015 год).

Приложение А и Б содержит подробную статистику об орбитах относительно группы Джевонса и её подгрупп для функций 1 – 5 аргументов.

Приложение В и Г содержит полученные результаты в ходе численных экспериментов при использовании основного алгоритма анализа джевонс-эквивалентности данных.

По теме диссертации опубликовано 14 печатных работ, среди которых 4 статьи в изданиях, входящих в перечень ВАК РФ и 2 свидетельства о регистрации программ в Государственном реестре регистрации программ для ЭВМ.

Содержание работы изложено связанно и последовательно. Каждая последующая глава опирается на результаты предыдущей. По каждой главе сделан вывод и заключение содержит общий вывод по результатам исследования.

Научная новизна и значимость полученных результатов

Соискателем заявлены следующие новые результаты:

– найдены два эффективных представления группы Джевонса для задания действия над БВ и БФ, которые позволяют снижать трудозатраты при разработке моделей программных систем, основанных на этом действии;

– исследованы действия элемента группы Джевонса над БФ, и в результате найдены новые частотные свойства этих действий. Такие свойства позволяют разрабатывать и исследовать алгоритмы анализа данных, основывающиеся на их частотных (энтропийных) характеристиках;

– найдено новое каноническое представление элемента группы Джевонса, и на его основе создан эффективный алгоритм решения уравнения действия такого элемента над БФ. Он позволяет решить проблему поиска элементов группы, связывающих джевонс-эквивалентные данные;

– введено новое понятие эквиморфизма групп, доказано эквиморфное вложение группы Джевонса в симметрическую группу степени 2^n. На его основе разработан эквиморфный вычислитель, являющийся моделью архитектуры процессора, на котором могут создаваться новые программные системы обработки данных. Он включает в себя эффективные алгоритмы вычисления действия элемента группы Джевонса над БФ.

Пункты новизны фактически отражают содержимое соответственных глав работы. Заявленные пункты действительно являются новыми результатами, но при этом их ценность не равнозначна. Первый пункт о представлениях группы Джевонса, несмотря на то, что предложенный автором метод (как и сами результаты – представления группы Джевонса) новый, все же является детальным и скрупулезным описанием предметной

области и не содержит качественно нового математического результата. Последний пункт об эквиморфном вычислителе является новым, но заявленные в нём результаты носят скорее техническую новизну, потому что полученные результаты позволяют линейно снизить сложность предложенного соискателем в третьей главе основного алгоритма. Предложенный метод эффективного анализа джевонс-эквивалентности данных позволяет не только продолжать теоретические изыскания в этом направлении, но и охватывает ряд новых теоретических результатов. К ним можно отнести найденные частотные свойства действия элементов группы Джевонса над булевыми функциями. Эти свойства имеют перспективу для использования в разработках методов анализа алгоритмов, предназначенных для обработки информации. Отдельно стоит выделить, что основной результат исследования – эффективный алгоритм анализа джевонс-эквивалентности данных непосредственно может быть использован в криптографии и криптологии в шифрах, которые используют действие группы Джевонса над функциями в качестве криптографического примитива. Предложенная модель эквиморфного вычислителя непосредственно может быть использована для создания автоматизированных средств обработки информации, использующих действия группы Джевонса над булевыми функциями.

Достоверность результатов

Все приведенные в диссертации теоретические результаты имеют математические доказательства. В части обоснования эффективности предложенного основного алгоритма проведены компьютерные эксперименты, показывающие, что в подавляющем большинстве случаев он эффективен. При этом даны оценки границ применимости, опирающиеся на теорию перечислений Пойа.

Результаты работы представлялись на конференциях международного уровня и обсуждались на специализированных семинарах (Москва, Красноярск, Новосибирск). Труды этих конференций рецензируются. Основные результаты опубликованы в 4 статьях в рецензируемых изданиях, рекомендованных ВАК.

Соответствие темы диссертации заявленной научной специальности

Диссертационное исследование соответствует паспорту специальности 05.13.17 – Теоретические основы информатики по следующим пунктам:

– пункт 5 «Разработка и исследование моделей и алгоритмов анализа данных»;

– пункт 14 «Разработка теоретических основ создания программных систем для новых информационных технологий».

Замечания

При рассмотрении диссертационной работы выявлен ряд недостатков и замечаний:

а) соискатель применяет обратную нотацию для обозначения аргументов булевых функций и нумерует аргументы от нуля, т.е. $f(x_{n-1},\dots,x_0)$ в противовес общепринятому математическому обозначению $f(x_1,\dots,x_n)$. Несмотря на то, что применяемая соискателем нотация удобна при компьютерных реализациях алгоритмов, она не является общепринятой и читателю требуется время для адаптации к такой системе обозначений;

б) введённое в главе 2 (стр. 45) понятие определенной эквивалентности групп, названной «Эквиморфизмом», и последующее доказательно эквиморфизма групп Джевонса и подгруппы симметрической группы $S_{2\hat{}n}$ оказалось безусловно полезным при разработке и компьютерной реализации алгоритмов и может оказаться перспективным для дальнейших исследований. При этом стоит подчеркнуть, что понятие эквиморфизма отражает суть установления связи между двумя группами по эквивалентному действию на одном и том же множестве. В силу того, что понятие «эквиморфизм» не сводимо к понятию «изоморфизм», требуется детальная проработка свойств эквиморфизмов в рамках последующих работ при исследовании действий групп на множествах;

в) замечание по терминологии. Предложенный термин «эквиморфизм» уже занят, употребляется для обозначения гомеоморфизма определенного типа. Введенное соискателем понятие эквивалентности групп относительно действия на множестве является новым, неплохо было бы в дальнейшем использовать новый термин для избегания коллизий и лучшей ассоциации с определяемой групповой эквивалентностью;

г) предложенный в третьей главе диссертации основной алгоритм решения уравнения действия группы Джевонса над булевыми функциями относительно неизвестного действующего элемента не имеет доказательства полиномиальной сложности. Приведённые в четвёртой главе различные подходы и, особенно, компьютерные эксперименты для оценки его сложности позволяют говорить о **предположительно** полиномиальной сложности предложенного алгоритма для подавляющего большинства булевых функций (с тривиальной подгруппой инерции);

д) предложенная соискателем модель эквиморфного вычислителя в третьей главе, содержащая три алгоритма действия позволяет повысить производительность вычислений при анализе джевонс-эквивалентности данных. Однако при вычислении действий произвольного элемента группы Джевонса над булевой функцией появляются сомнения в приросте производительности в тысячи раз. Несмотря на то, что данная задача не является ключевой в диссертационной работе, все же требуется исследовать возможность применения (возможно с модификацией) эквиморфного вычислителя для реализации действий произвольными элементами группы Джевонса над булевой функцией;

е) изложение математических аппаратов перегружено предлагаемыми соискателем примерами. Несомненно, примеры существенно упрощают работу программиста при компьютерной реализации соответствующих алгоритмов, но при этом могут быть убраны из работы без значительного ущерба для последней;

ж) каноническое представление элемента группы Джевонса, существование которого доказано в теореме 3.1 возможно только для представлений, заданных формулами (10.А) и (10.Б) на стр. 32. Стоило об этом упомянуть.

Заключение

Диссертация соответствует специальности 05.13.17 – Теоретические основы информатики, изложена целостно и является законченной научно-квалификационной работой, в которой на основании выполненных соискателем исследований содержится решение задачи эффективного анализа джевонс-эквивалентности данных, имеющей существенное значение для теоретической информатики и кибернетики. Работа выполнена соискателем самостоятельно на высоком научно-техническом уровне. Полученные результаты достоверны. По каждой главе и работе в целом сделаны обоснованные выводы. Автореферат полностью соответствует содержанию диссертации.

Отмеченные недостатки не носят принципиального характера и не умоляют ценности полученных соискателем теоретических и практических результатов.

Считаю, что диссертационная работа отвечает требованиям п. 9 «Положения о порядке присуждения учёных степеней» постановления Правительства Российской Федерации от 24.09.2013 г. № 842, а её автор Кукарцев Анатолий Михайлович заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

Доктор физико-математических наук, профессор,
профессор кафедры Алгебраических
и информационных систем
ФГБОУ ВО «Иркутский
государственный университет» Винокуров Сергей Федорович

Подпись С. Ф. Винокурова заверяю:

ФГБОУ ВО «ИГУ»
ПОДПИСЬ УДОСТОВЕРЯЮ
Специалист по кадрам
Е.И. Чупрунова
«21» марта 2017 г.

21.03.2017
г. Иркутск, б. Гагарина, 20
Кабинет № 234
e-mail: imei@math.isu.ru
р.т. 83952521298