«УТВЕРЖДАЮ»

Проректор по научной работе НИУ «МЭИ»

д.т.н. В. К. Драгунов _____

6.02 2014 г.

Отзыв ведущей организации
на диссертацию Лысикова Владимира Владимировича
“Некоторые вопросы теории сложности билинейных отображений”,
представленную на соискание учёной степени кандидата
физико-математических наук по специальности 01.01.09 –
дискретная математика и математическая кибернетика

Актуальность темы диссертации

В обсуждаемой диссертации анализируется сложность одного класса алгоритмов, предназначенных для вычислений в различных алгебраических структурах с операциями сложения и умножения.

Теория сложности алгоритмов --- один из важнейших разделов дискретной математики и математической кибернетики. Поведение всех искусственных и многих естественных управляющих систем осуществляется по определенным алгоритмам. Алгоритмы постоянно совершенствуются в ходе естественного отбора, конкуренции и эволюции, под воздействием целенаправленного изменения разработчиками искусственных систем, отвечающими на запросы пользователей. Общепризнанными критериями качества алгоритмов являются различные показатели их сложности, формулируемые и оцениваемые математическими средствами, среди которых наибольшее значение приобретают модели и методы дискретной математики (так как любой алгоритм состоит из конечного числа элементарных шагов). Различные особенности алгоритмов и способов их реализации должны быть учтены адекватными этим особенностям критериями сложности, для улучшения таких показателей сложности применяется соответствующий математический аппарат.

Важным и, как оказалось, эффективным и достаточно общим методом вычислений и, следовательно, реализации алгоритмов являются билинейные и полилинейные отображения. Они применяются, в частности, в задачах

умножения матриц и полиномов над различными кольцами конечной, счетной и несчетной мощности. Другой областью применения полилинейных отображений может стать анализ замкнутых классов в различных функциональных системах, содержащих линейные функции, как дискретных, так и непрерывных. Полилинейные алгоритмы --- один из способов суперпозиции и, следовательно, вычисления функций, при этом возможны и весьма эффективны параллельные вычисления.

Практические задачи обеспечения информационной безопасности часто решаются путем введения и анализа различных показателей нелинейности дискретных функций. Билинейные отображения и оценки их сложности вполне применимы и для решения таких задач.

Отметим также, что анализ сложности полилинейных отображений способствует решению и сугубо теоретических проблем, в частности, в алгебре, о чем свидетельствуют и некоторые результаты данной диссертации.

Указанные соображения обосновывают актуальность темы обсуждаемой работы, ее теоретическое и практическое значение.

Научная новизна исследования и его результатов

Основные результаты автора работы изложены в главах 2-4 после обоснования темы исследования, убедительного исторического обзора и предварительных сведений и состоят в следующем.

1. Установлена структура оптимальных алгоритмов для частного случая билинейных отображений, ранг (сложность) которых равен сумме размерностей пространств-аргументов: алгоритмы должны быть двухкомпонентными (лемма 2.1), а пространства должны обладать базисами особого вида (теорема 2.4).

2. Найдено необходимое и достаточное условие для того, чтобы билинейная сложность локальной алгебры отличалась от оптимальной на 1 (алгебра «почти оптимальна») --- теорема 2.6. Доказано, что почти оптимальными являются алгебры обобщенных кватернионов, сконструированы почти оптимальные алгоритмы умножения в таких алгебрах (теоремы 2.7 и 2.8).

3. Уточнена известная ранее (М. Блезер, 2003) оценка сложности умножения в матричных алгебрах (теорема 3.5), что позволило описать все почти оптимальные полупростые алгебры (теорема 3.6).

4. Доказано, что ранги **Z**–билинейного отображения над бесконечными и конечными алгебраически замкнутыми расширенными полями совпадают всегда кроме, возможно, конечного числа значений ненулевой характеристики поля (теорема 4.1).

Все эти результаты являются новыми и получены автором самостоятельно.

Значимость результатов диссертации для науки и производства

Результаты проведенного исследования обогащают теорию сложности алгоритмов. Они обобщают и уточняют ранее полученные результаты и могут послужить основой дальнейшего развития теории.

Выявлены особенности оптимальных и почти оптимальных билинейных отображений во многих частных случаях, найдены аналогии и общие черты оптимальных отображений над различными алгебраическими структурами.

Завершено описание всех почти оптимальных полупростых алгебр, начатое в 2009 г. М. Блезером и А. де Вольтером в частном случае, когда в качестве поля берется **R**. В их работе важную роль сыграло кольцо кватернионов, причем их подход не допускал обобщения; завершению этих исследований способствовали оригинальные идеи и результаты данной диссертации (теоремы 2.7, 2.8) об алгебрах обобщенных кватернионов.

Результаты диссертации можно применить и в теории функциональных систем (многозначной логики, системах полиномов над конечными и бесконечными кольцами) для описания замкнутых классов, содержащих линейные функции, для построения эффективных алгоритмов реализации функций каноническими формулами, для вычисления значений функций и распознавания их свойств, поиска полных систем и анализа решетки замкнутых классов.

Билинейные отображения и результаты об их сложности открывают широкие возможности распараллеливания процессов и вычислений, совершенствованию методов обработки информации и ее защиты, оценки актуальных с точки зрения криптологии характеристик дискретных функций и их классов.

Выявлены новые приложения алгебраических методов в задачах дискретной математики и теоретической информатики. Приведенные два доказательства теоремы 4.1 (одно --- лаконичное и изящное, выполненное средствами метаматематики), являются методологически важным подтверждением глубокой связи различных разделов математики, алгебры и логики.

Результаты диссертации могут найти применение в научных и образовательных учреждениях, занимающихся теорией сложности алгоритмов и их практическим применением, в частности, Московском, Новосибирском, Иркутском, Санкт-Петербургском госуниверситетах, Сибирском федеральном университете, ВЦ им. А.А. Дородницына РАН, ИПМ им. М. В. Келдыша РАН, Институте математики им. С. Л. Соболева СО РАН, ИСП РАН, НИУ «МЭИ», МГТУ им. Н.Э. Баумана, ООО «Яндекс» и др.

Представляются уместными следующие **критические замечания**.

1. В тексте диссертации не приведена формулировка теоремы Блезера и де Вольтера о полупростых алгебрах минимального ранга над полем **R** и роли кольца кватернионов при их характеризации. Включение этой теоремы в текст придало бы больше полноты историческому обзору и обоснованию исследования сложности умножения в алгебрах обобщенных кватернионов. (Следует отметить, что этот результат автору хорошо известен и приведен в автореферате на с. 4.)

2. При описании основных результатов главы 4 в вводных частях работы неточно передается смысл теоремы 4.1, не указывается разница между нулевой и ненулевой характеристикой поля.

3. При цитировании результатов Баура и Штрассена (теоремы 1.3, 1.4) не поясняются некоторые обозначения.

Как пожелание, а не замечание отметим, что изложение стало бы более прозрачным при иллюстрации многочисленных алгебраических конструкций известными понятиями и результатами из области дискретной математики.

Приведенные замечания не носят принципиальный характер и не влияют на оценку работы по существу.

Автореферат верно и полно отражает содержание диссертации. Результаты исследования опубликованы и доложены на научных конференциях и семинарах.

Таким образом, диссертационная работа Владимира Владимировича Лысикова “Некоторые вопросы теории сложности билинейных отображений” представляет собой законченное научное исследование, содержащее новые результаты в теории сложности алгоритмов, и удовлетворяет всем требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 01.01.09 – дискретная математика и математическая кибернетика.

Отзыв утвержден на заседании кафедры математического моделирования Московского энергетического института 31 января 2014 г., протокол № 6.

Заведующий кафедрой
математического моделирования НИУ «МЭИ»
докт. физ.-мат. наук, профессор А. А. Амосов

Канд. физ.-мат. наук, доцент Д. Г. Мещанинов