



УТВЕРЖДАЮ

Директор ФГУП «НИИ «КВАНТ»,
академик АК РФ, д.т.н., с.н.с


23 

Г.С. Елизаров



ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

о диссертационной работе Лапикова Игоря Игоревича «Построение и реализация алгоритмов решения систем целочисленных неравенств в методе разделяющих плоскостей», представленной на соискание ученой степени кандидата технических наук по научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Актуальность и новизна темы диссертации

Разработка и внедрение новых алгоритмов решения задач дискретной математики представляет повышенный интерес и является актуальной как для прикладных областей их возможного практического внедрения, так и для вычислительной сферы с точки зрения логической организации процессов с наилучшими сложностными характеристиками.

Построенный в диссертации Лапикова И.И. алгоритм решения систем линейных неравенств относительно дискретных неизвестных безусловно является таковым. В его структуре сочетаются рациональные идеи метода эллипсоидов и вместе с тем алгоритм, предложенный Хачияном, корректируется с целью нахождения на конечном этапе не действительных, как было в его исходной редакции, а непосредственно целочисленных решений. В результате разработанный автором новый адаптивный алгоритм эллипсоидов может быть

применен для широкого круга практических задач, в том числе в области информационной безопасности, например, при анализе генераторов псевдослучайных последовательностей. Сама возможность его применения в этих задачах является новой, и автор значительное внимание уделяет рассмотрению возникающих практических приложений.

С вычислительной точки зрения проблема реализации исходного алгоритма Хачияна и построенного в диссертации адаптивного алгоритма также обладает очевидными чертами новизны, отличающими эти алгоритмы от традиционных, в частности алгоритмов решения систем линейных уравнений. Главное различие связано с нахождением на каждой итерации алгоритма квадратичных форм, задающих текущий эллипсоид (в отличие от операций с линейными формами в методах решения систем линейных уравнений). Работа с квадратичными формами требует специфической организации вычислительной среды, при этом итеративная структура нового алгоритма эллипсоидов и однотипные операции на каждом шаге дают возможность предложить рациональные схемы реализации вычислительного процесса. Кроме того, все функции в рамках алгоритма, имеют степень нелинейности, не превосходящую двух, что также позволяет сделать вывод о возможности реализации алгоритма эллипсоидов с приемлемой сложностью при сравнительно больших размерах исходной задачи.

Достоверность полученных результатов и выводов

В представленной диссертации сочетаются теоретические и экспериментальные методы исследования.

Достоверность теоретических положений достигается построением и исследованием адекватных математических моделей. Корректность экспериментальных выводов обеспечивается практической реализацией разработанных алгоритмов на ЭВМ с получением результатов, согласующихся с теоретиче-

скими оценками. Дополнительное обоснование достоверности экспериментальных результатов подтверждается актами о внедрении и полученными свидетельствами о регистрации программ для ЭВМ.

Общая оценка работы

Диссертация состоит из введения, трех глав, заключения, списка литературы и приложений.

Во введении дан краткий обзор тематики диссертации, обоснована ее актуальность, перечислены цели и задачи, которые стояли перед автором в процессе исследования, приведены формулировки новых результатов, полученных автором и выносимых на защиту, обоснована теоретическая и практическая значимость развития выбранной области исследований.

Первая глава посвящена проблематике псевдобулевого направления в дискретной математике. В параграфе 1.1 рассмотрены свойства пороговых функций, задаваемых линейными неравенствами в действительной области. В параграфе 1.2 проведен обзор направлений развития методов анализа и решений произвольных систем булевых уравнений. В параграфе 1.3 изучены способы представления дискретных задач в пороговом базисе, проанализированы результаты Балакина Г.В., Никонова В.Г. в разработке метода разделяющих плоскостей и метода разделяющих поверхностей.

Во второй главе на основе глубокого изучения метода эллипсоидов и алгоритма Хачияна автором построены новые алгоритмы решения систем целочисленных неравенств. В параграфе 2.1 проведен анализ концепции построения полиномиального алгоритма Хачияна. В параграфе 2.2 обобщены положения метода эллипсоидов, выделены необходимые процедуры для его применения в k -значной области. На базе проведенного анализа в параграфе 2.3 построен адаптивный алгоритм эллипсоидов решения систем линейных неравенств с k -значными неизвестными, обоснована его сходимость и определены условия его применения. В параграфе 2.3 описана модификация адаптивного алгоритма на базе декомпозиции области поиска решений с возможностью

распараллеливания алгоритма на ЭВМ. В параграфе 2.4 проведено сравнение параметров работы предложенного алгоритма с альтернативными.

В третьей главе внимание уделено изучению возможностей применения разработанных алгоритмов в прикладных задачах анализа узлов защиты информации и дискретной математики. В параграфе 3.1 проведен обзор основных направлений применения генераторов псевдослучайных последовательностей (ПСП) в современных системах обеспечения информационной безопасности. В параграфе 3.2 рассмотрена задача изучения запретов и полужапретов булевых и k -значных функций, показана возможность применения адаптивного алгоритма при их построении. В параграфе 3.3 разработанные алгоритмы использованы в задачах анализа биективных отображений. В параграфе 3.4 адаптивный алгоритм эллипсоидов для восстановления начального состояния ряда типовых узлов защиты информации. В параграфе 3.5 описан полиэдральный метод восстановления линейной рекурренты над кольцом \mathbb{Z}_2^m по ее старшей координатной последовательности, получена эмпирическая оценка расстояния единственности задачи. В параграфе 3.6 проведено исследование возможности применения метода эллипсоидов для распознавания и нахождения аналитического задания пороговой k -значной функции и доказано, что эта задача в общем случае имеет полиномиальную сложность.

В заключении диссертации подведены ее итоги и намечены некоторые направления дальнейших исследований.

В работе автор применяет алгебраические, комбинаторные, теоретико-автоматные методы, включая использование теории k -значных функций и линейного программирования.

Следует отметить стиль изложения материалов: последовательность, хороший язык, наличие поясняющих примеров, минимальное количество опечаток – все это облегчает восприятие диссертации.

Основные положения в достаточной степени апробированы и отражены в научной печати, что подтверждается десятью публикациями, включавшими семь статей в журналах Перечня ВАК, и двумя свидетельствами о регистрации

программ для ЭВМ. Результаты диссертации докладывались и обсуждались на семинарах, а также на международных и всероссийских конференциях. О практической значимости свидетельствуют полученные акты о внедрении результатов диссертации в работу трех профильных учреждений.

Значимость полученных автором результатов

В диссертации разработан новый алгоритм решения систем линейных неравенств с k -значными неизвестными, который расширил арсенал методов анализа и решения систем нелинейных дискретных уравнений. Новый адаптивный алгоритм построен на базе полиномиального алгоритма эллипсоидов Хачияна и для некоторых практически важных классов систем сохранил полиномиальную оценку сложности.

Указан способ геометрического распараллеливания нового адаптивного алгоритма на t потоков со снижением его временной сложности.

В диссертации новый адаптивный алгоритм применен в задачах анализа узлов защиты информации, включающих генераторы ПСП, и показал свою практическую эффективность.

В задаче восстановления линейной рекурренты над кольцом \mathbb{Z}_2^m по отрезку подряд идущих знаков старшего разряда новый алгоритм не только показал свою применимость, но и позволил вывести эмпирическую оценку расстояния единственности.

С применением метода эллипсоидов показано, что задача распознавания пороговой k -значной функции имеет полиномиальную сложность.

Результаты диссертации могут быть использованы в научных центрах, занимающихся анализом систем защиты информации, в частности, генераторов ПСП. Кроме того, положения и результаты диссертации могут быть использованы при решении различных задач информационной безопасности, сводимых к системам линейных неравенств с k -значными неизвестными. Учитывая, что диссертация тщательно проработана с методологической точки зре-

ния и содержит примеры, иллюстрирующие практическое применение ее положений при решении задач анализа ряда конкретных систем информационной безопасности, ее материалы целесообразно использовать в учебном процессе при подготовке студентов и аспирантов соответствующих специальностей, о чем, в частности, свидетельствует акт о внедрении в учебный процесс БФУ им. Канта.

Адаптивный алгоритм эллипсоидов, как универсальный метод решения систем линейных неравенств с дискретными неизвестными целесообразно в дальнейшем рассматривать в качестве одного из тестовых алгоритмов для оценки производительности вычислительных комплексов.

Замечания и пожелания по диссертации

1. В диссертации мало внимания уделено исследованию особенностей и сложностных параметров реализации разработанных алгоритмов на различных вычислительных платформах.

2. Диссертация бы выиграла, если бы в ней был указан способ синтеза генератора ПСП, для которого разработанные методы анализа неприменимы, либо их применение затруднительно ввиду высокой трудоемкости.

3. Предложенный в диссертации метод распараллеливания адаптивного алгоритма целесообразно было бы сопроводить более глубоким изучением временных и емкостных параметров с тем, чтобы более четко оценить выгоды от такого приема.

4. Представлялось бы полезным выделить центральную процедуру адаптивного алгоритма: построение эллипсоида минимального объема – и детально проанализировать ее реализацию с учетом возможностей оптимизации временной и емкостной сложностей.

Указанные недостатки существенно не влияют на итоговую ценность достигнутых результатов и общую высокую оценку научно-квалификационного уровня соискателя и могут быть учтены при выборе направлений дальнейшего развития соискателя.

Заключение

Представленная диссертационная работа на тему «Построение и реализация алгоритмов решения систем целочисленных неравенств в методе разделяющих плоскостей» является законченной научно-квалификационной работой, в которой решена актуальная и значимая научно-техническая задача. В ней предложены новые подходы к анализу систем защиты информации. Новые научные результаты вносят вклад в расширение арсенала алгоритмических методов современной дискретной математики и представляют как теоретический, так и практический интерес.

Работа соответствует критериям «Положения о порядке присуждения ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 №842), предъявляемым к кандидатским диссертациям, а ее автор Лапиков Игорь Игоревич заслуживает присуждения ученой степени кандидата технических наук по научной специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв составлен ученым секретарем ФГУП НИИ «КВАНТ», кандидатом технических наук, старшим научным сотрудником Яблонским С.В., обсуждён и одобрен на заседании научно-технического совета ФГУП «НИИ «КВАНТ» (протокол № 6/19 от 18 апреля 2019 г.)

Кандидат технических наук, старший научный сотрудник, (специальность 05.13.13 – «Телекоммуникационные системы компьютерные сети»)

Ученый секретарь ФГУП «НИИ «КВАНТ»

Тел. +74991539584

 Яблонский Сергей Валерьевич

«22» апреля 2019 г.

Подпись Яблонского С.В. заверяю


Начальник отдела кадров
ФГУП «НИИ «КВАНТ»
А. А. Рогожников

«22» апреля 2019 г.