ОТЗЫВ

официального оппонента на диссертацию Таранникова Юрия Валерьевича
«Конструкции и свойства корреляционно-иммунных и платовидных булевых функций»
на соискание ученой степени доктора физико-математических наук
по специальности 2.3.6 — методы и системы защиты информации,
информационная безопасность

Цель диссертационного исследования состоит в исследовании методов построения и свойств булевых функций с характеристиками, важными для использования функций в системах защиты данных, среди которых одну из центральных ролей играет корреляционная иммунность (в диссертации также часто используется термин «устойчивость», которая означает корреляционную иммунность плюс уравновешенность – одинаковое число нулей и единиц булевой функции).

Актуальность. Булевы функции – классические объекты теории информации и дискретной математики. Кроме работ по исследованию непосредственно классов булевых функций, на языке булевых функций или их обобщений формулируется множество задач комбинаторики и разработанный для таких функций аппарат часто бывает полезен для какой-то конкретной области либо явно, через представление рассматриваемых объектов булевыми функциями, либо в виде потенциальных обобщений результатов, полученных для булевых функций, на другие классы объектов. В качестве примеров последнего можно привести исследование кодов и схем (в англоязычной терминологии – дизайнов) в дистанционно регулярных графах (гиперкуб, на вершинах которого определяются булевы функции, является частным примером такого графа). Корреляционная иммунность булевых функций, являющаяся одним из центральных понятий, изучению которых посвящена диссертация Юрия Валерьевича Таранникова, это свойство, к которому как непосредственно сводятся важные характеристики комбинаторных объектов, так и в виде различных обобщений. Так, понятие дуального расстояния двоичного кода (не обязательно линейного) описывается через корреляционную иммунность его характеристической булевой функции, а для недвоичных кодов и кодов в других схемах, отличных от схемы Хэмминга, через обобщения этого понятия, при этом техника исследования также во многом является обобщенной техникой исследования для булевых функций. Иногда теория приобретает определенную замкнутость и получает мощное развитие именно в обобщенном виде, и в данном конкретном контексте булевы функции уже оказываются частным случаем, а не флагманом. Примером является теория Ф.Дельсарта, рассматривающая помехоустойчивые коды (двоичные коды по сути являются булевыми функциями с определенными метрическими свойствами) в общем контексте схем отношений.

С точки зрения вышесказанного, результаты Ю.В.Таранникова, представленные в диссертации, не только являются фундаментально значимыми для областей, связанных с практическим применением булевых функций, что хорошо разъяснено во введении диссертационной работы, но также имеют важное значение для актуальных теоретических направлений дискретной математики и алгебраической комбинаторики. Часть результатов уже оказала значительное влияние на области, непосредственно не связанные с булевыми функциями. Например, для корреляционно иммунных функций из класса, построенного в работах Юрия Валерьевича,

несбалансированных булевых функций с корреляционной иммунностью порядка 2n/3-1, найдены аналоги циркулянтных графах, бесконечных транзитивных решетках, дистанционно-регулярных графах Дуба.

Структура диссертации. Диссертация состоит из введения, семи глав, заключения и списка литературы из 189 источников. Общий объем диссертации составляет 287 стр. Во введении обоснована актуальность исследований, сформулирована их цель, описаны методы исследования, дана общая характеристика работы, сформулированы основные результаты.

В первой главе диссертации вводятся основные определения и понятия, принятые в литературе по булевым функциям и используемые в диссертации, приведены известные базовые результаты (во многих случаях для полноты изложения приведены доказательства в изложении диссертанта). В этой же главе доказан один из основных результатов диссертации – оценка нелинейности булевой функции при данном порядке корреляционной иммунности (отдельно для уравновешенных функций, включая улучшение для функций, не достигающих границы Зигенталера, и для неуравновешенных функций).

Во второй главе разработаны конструкции уравновешенных корреляционно-иммунных (то есть устойчивых) булевых функций, достигающих границы нелинейности, доказанной в первой главе. Приведено несколько конструкций, каждая из которых имеет свой диапазон параметров (число аргументов, порядок корреляционной иммунности), не покрываемый другими конструкциями. Также рассмотрены вопросы схемной реализации построенных булевых функций, что имеет прямое отношение к возможности их практического использования, например в качестве нелинейного фильтра в поточных шифрах на основе регистра сдвига с линейной обратной связью.

В третьей главе исследуются различные характеристики корреляционно-иммунных булевых функций. Одной из важнейших с практической точки зрения характеристик является автокорреляция, определяемая как максимальное отклонение веса производной функции от среднего. В работе доказано улучшение известной нижней оценки Зенга и Занга автокорреляции булевой функции заданного порядка корреляционной иммунности. Другой важной характеристикой является число нелинейных аргументов функции. Автором показано, что функция корреляционной иммунности порядка n-k, где k – константа, может зависеть нелинейно не более чем от p(k) аргументов, где p(k) не зависит от n. Фактически это означает, что число классов эквивалентности таких функций ограничено и не зависит от n, если n>p(k). Приведены также верхняя и нижняя оценки на величину p(k), указывающие на ее экспоненциальный рост. Отмечено, что данные исследования перекликаются с исследованиями других ученых числа существенных аргументов булевой функции ограниченной степени (над полем вещественных чисел), задачи сводятся одна к другой. При этом исследования по функциям ограниченной степени проводились независимо и примерно в то же время, в части результатов отставая от работ соискателя (на данный момент известные результаты по корреляционно иммунным функциям и функциям ограниченной степени существенно дополняют друг друга, несмотря на частичное пересечение). Следующий результат диссертации (раздел 3.6) как раз и сформулирован в терминах такой «вывернутой» постановки, рассматриваются так называемые с-регулярные булевы функции, которые по сути являются булевыми функциями, представимыми (над R) однородным

многочленом степени c. Сами по себе они являются корреляционно иммунными функциями порядка c-1, но при инвертировании значения функции на четных наборах аргументов превращаются в корреляционно иммунные функции порядка n-c-1, и результаты по числу существенных аргументов такой функции можно трактовать в терминах числа нелинейных аргументов «вывернутой» функции. Оценки при этом получаются лучше, чем в предыдущем параграфе, поскольку используется регулярность функции.

В четвертой главе исследуется ранг платовидной функции. Платовидные функции – булевые функции, преобразование Уолша которых принимает только три значения -A, 0, A. В частности, функции, на которых достигается оценка, связывающая нелинейность булевой функции с порядком ее корреляционной иммунности, являются платовидными. Ранг – это размерность аффинного замыкания носителя (множества ненулей) преобразования Уолша данной функции. Приведены оценки на ранг платовидной функции с данной мощностью носителя преобразования Уолша и конструкции платовидных функций разного ранга с данной мощностью носителя. В частности, получена характеризация возможных значений ранга для носителя мощности 16.

В пятой главе рассматривается построение разбиения пространства над конечным полем на аффинные подпространства. С темой диссертационного исследования эта тема связана известными конструкциями платовидных функций (в частности, бент-функций), в которых используются разбиения пространства, однако изучение подобных разбиений является также естественным направлением в тренде современных исследований в конечных геометриях. Приведены оценки на основные параметры разбиения (размерность пространства, размерность подпространств, порядок поля), при которых существуют нередуцируемые разбиения, и оценки на число разбиений пространства на аффинные подпространства.

В шестой главе рассматриваются некоторые естественные комбинаторные обобщения понятия корреляционно-иммунной булевой функции. Вместо равномерного распределения значений функции по граням заданной размерности от функции требуется «почти равномерная» распределенность по граням любой размерности или шарам любого радиуса. Техника исследования подобных объектов сильно отличается в сторону меньшей алгебраичности и большей комбинаторной изощренности, поскольку «почти равномерная» распределенность не описывается линейными уравнениями. Одним из центральных результатов главы является описание возможных асимптотических пределов значений плотности функций, равномерно уравновешенных по граням.

В седьмой главе рассмотрены инвариантные классы булевых функций и доказан критерий бесконечности инвариантного класса, заданного набором запрещенных подфункций. Заметим, что корреляционно иммунные функции образуют класс булевых функций, инвариантный относительно взятия подфункций, хотя область применимости результатов седьмой главы гораздо шире.

Значимость полученных результатов. Теоретическая значимость исследования состоит в получении ответов на фундаментальные вопросы теории булевых функций, связанные с их основными характеристиками, важными для приложений в области информационной безопасности и защиты данных. Многие полученные автором результаты, а также методы комбинаторного анализа, в частности анализа преобразования Уолша булевых функций, хорошо

известны среди отечественных и зарубежных специалистов и получили развитие в работах других ученых, входят в курсы по дискретной математике для студентов математических и IT-специальностей ведущих вузов страны.

Результаты диссертации, выносимые на защиту, являются новыми и снабжены строгими математическими доказательствами. Основные результаты работы опубликованы в 20 статьях в изданиях, входящих в перечень рецензируемых научных журналов, в которых должны быть опубликованы основные результаты диссертации на соискание ученых степеней доктора и кандидата наук. Результаты, вошедшие в диссертацию, прошли широкую апробацию, докладывались на многочисленных международных и российских научных конференциях и семинарах.

Автореферат правильно и полно отражает содержание диссертации.

Замечания. Имеются несогласования форм частей предложения, например, на с. 9 «получения критерия, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, и определения, содержит ли этот класс бесконечное число существенно разных функций» (по-видимому, имеется ввиду «…, позволяющего по … определить, содержит ли …»), на с. 15 «В параграфе ... из двух функций … строятся две новых» (правильно «две новые»), на с.151 «Автор рассмотрел …, даем …».

С.6 «Следствие 1.7 утверждает, что m-устойчивые булевы функции от n переменных обязаны одновременно быть платовидными.» Здесь автор забыл упомянуть нелинейность, без которого утверждение теряет смысл (который, конечно, легко восстановить по формулировке Следствия 1.7).

Во введении на с.26 при цитировании теоремы 5.14 не определено обозначение $c_q(m,n)$.

В главе 3 хорошо комментируется связь корреляционно-иммунных булевых функций с функциями ограниченной степени (над R) при помощи простой операции, которую для краткости здесь назовем «выворачиванием». Однако в разделе 3.6 как раз приводится оценка на число существенных переменных, которую можно трактовать как оценку числа существенных аргументов для функций ограниченной степени специального вида (регулярных), что при «выворачивании» дает результат в терминах предыдущего раздела (оценку числа нелинейных аргументов для регулярных функций высокого порядка корреляционной иммунности). Это важное и естественное в контексте общей тематики диссертации следствие не отмечено.

Указанные замечания никак не умаляют теоретической и практической значимости результатов диссертационной работы. В целом хочется отметить аккуратное оформление текста, и ориентированный на читателя стиль изложения, в чем по-видимому сказался большой преподавательский опыт Юрия Валерьевича. В частности, очень понятно, кратко, без излишеств, и в то же время математически строго во введении изложен пример применения корреляционно-иммунных функций в системах защиты данных.

Диссертация Юрия Валерьевича Таранникова на тему «Конструкции и свойства корреляционно-иммунных и платовидных булевых функций» имеет внутреннее единство, обладает новизной и является завершенной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны теоретические положения, совокупность которых можно квалифицировать как научное достижение в дискретной математике,

теории и методологии обеспечения информационной безопасности и защиты данных. Результаты диссертационного исследования Ю. В. Таранникова соответствуют паспорту научной специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Диссертация соответствует критериям, определенным в пп. 2.1–2.5 «Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», предъявляемым к докторским диссертациям, а ее автор, Таранников Юрий Валерьевич, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
доктор физ.-мат. наук, профессор РАН
Кротов Денис Станиславович,
главный научный сотрудник
Федерального государственного бюджетного учреждения науки Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук
Почтовый адрес: Российская федерация, Новосибирск, 630090, пр. Академика Коптюга, 4.
E-mail: krotov@math.nsc.ru
Телефон: +7(383)3297542

12 сентября 2023г.

Подпись Д. С. Кротова заверяю: