Тема работы: Регулярные разбиения 12-куба с параметрами [[2,10],[6,6]]

Кротов Денис Станиславович, г.н.с. ИМ СО РАН, д.ф.-м.н.
(по совместительству преподаватель НГУ)

Аннотация

В работе классифицированы с точностью до эквивалентности регулярные разбиения 12-куба с фактор-матрицей $[[2,10],[6,6]]$, или, что то же самое, простой ортогональный массивы $\mathrm{OA}(1536,12,2,7)$ или корреляционно-иммунное логическое значение 7-го порядка функций от 12 переменных с 1536 единицами (что завершает классификацию несбалансированных корреляционно-иммунных булевых функций порядка 7 от 12 переменных). Установлено, что существует 103 класса эквивалентности рассматриваемых объектов, среди них всего два почти-OA(1536,12,2,8). Дополнительно, установлена единственность с точностью до эквивалентности ортогонального массива $\mathrm{OA}(1536,13,2,7)$.

Работа выполнена за счет гранта РНФ 18-11-00136 «Существование совершенных кодов и трейдов» 2018-2020, рук. Кротов Д.С.

1. Постановка задачи.

В работе исследуются экстримальные объекты дискретной математики, которые могут быть определены несколькими эквивалентными способами. Мы начнем с определения через булевы функции. $\{0,1\}$-значная функция от n аргументов, принимающих значения 0 или 1, называется булевой функцией. Булева функция называется корреляционно иммунно порядка t, если ее значение статистически независимо от значений любых t ее аргументов. Другими словами, если функция имеет M единиц среди значений на всех 2^n наборов значений аргументов, то зафиксировав любые t аргументов (одним из 2^t наборов значений), и пробегая все возможные значения оставшихся аргументов, мы получим $M/2^t$ единиц на выходе. В работе "A bound on correlation immunity" 2007 года (Сиб. электрон. матем. изв., том 4, с. 133-135) Д.Г.Фон-Дер-Флаасс доказал, что порядок корреляционной иммунности несбалансированной (то есть число нулей отлично от числа единиц) булевой функции от n аргументов, отличной от константы (везде 0 или везде 1), не может превышать $2n/3-1$. Более того, любая булева функция, порядок корреляционной иммунности которой лежащит на этой границе, соответствует регулярной структуре в булевом n-кубе, известной как регулярное разбиение (equitable partition), или совершенная раскраска (строгое определение будет дано в разделе 3). В работе решается задача

классификации с точностью до эквивалентности несбалансированных булевых функций от 12 аргументов с 1536 единицами и корреляционной иммунностью порядка 7, лежащей на границе Фон-Дер-Флаасса. Дополнительно рассмотрена задача классификации булевых функций от 13 аргументов с 1536 единицами и корреляционной иммунностью порядка 7, так как они соответствуют ортогональным массивам с параметрами OA$(1536, 13, 2, 7)$, а в проекции по одному направлению дают функции от 12 аргументов из рассматриваемого класса.

2. Современное состояние проблемы.

Теории корреляционно иммунных функций посвящено большое количество литературы. С точки зрения криптографических приложений наиболее интересны сбалансированные функции. Несбалансированные корреляционно иммунные функции важны для теории ортогональных массивов (по сути, они эквивалентны простым, то есть без повторений, двоичным ортогональным массивам OA$(M, n, 2, t)$), которые исследуются как в связи с применениями в теории статистического эксперимента, так и в связи с теоретическим интересом и связями с другими разделами математики. По классификации несбалансированных булевых функций с корреляционной иммунностью $2n/3 - 1$ ранее было известно следующее. При $n = 3$ такая функция одна с точностью до эквивалентности, она принимает значение 1 на двух противоположных наборах аргументов, например, $(0, 0, 0)$ и $(1, 1, 1)$, см. иллюстрацию в разделе 5. При $n = 6$ таких функций две, одна, с 16 единицами, получается рекурсивной конструкцией из функции для $n = 3$, вторая, с 24 единицами, также единственная с точностью до эквивалентности, была построена Ю. Таранниковым [Yu. Tarannikov. On resilient Boolean functions with maximal possible nonlinearity. Cryptology ePrint Archive 2000/005, 2000. `https://eprint.iacr.org/2000/005`]. Несбалансированные булевы функции от 9 переменных с корреляционной иммунностью 5 были описаны учеником Ю. Таранникова Д. Кириенко [D. Kirienko. On new infinite family of high order correlation immune unbalanced Boolean functions. In Proceedings 2002 IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30 – July 5, 2002, p. 465. IEEE, 2002], который показал, что существует ровно два класса эквивалентности таких объектов (число единиц 128). Размерность $n = 12$ оказалась очень интересной. Рекурсивная конструкция позволяла, стартуя с функций при $n = 3$ и $n = 6$, построить функции с 1024 и 1536 единицами и корреляционной иммунностью 7. Д.Г.Фон-Дер-Флаасс в работе [Совершенные 2-раскраски 12-мерного куба, достигающие границы корреляционной иммунности. Сиб. электрон. матем. изв., 2007, т. 4, с. 292-295] построил булевы функции от 12 аргументов с корреляционной иммунностью 7 и 1792 единицами и показал, что другого числа единиц, кроме 1024, 1536, 1792, у несбалансированных булевых функций от 12 аргументов с корреляционной иммунностью 7 быть не может. Таким образом, функции на рассматриваемой границе были классифицированы с точностью до параметров до 12 аргументов, и с точностью до эквивалентности до 9 аргумнтов. В недавней работе [On unbalanced Boolean functions with best correlation immunity. Electron. J. Comb. 21(1) 2020, P1.45(1-24)] К.Воробьёв и Д.Кротов в результате комбинирования теоретического и вычислительного подхода

охарактеризовали булевые функции от 12 аргументов с корреляционной иммунностью 7 и числом единиц 1024 и 1792. Подходы использовались разные, и ни один из них не подошел для числа единиц 1536, этот случай требовал дополнительного исследования, которое и было проведено в рамках данного проекта.

Отметим также, что данная работа связана с темой классификации ортогональных массивов (точнее, напрямую относится к этой теме), которой посвящена серия исследований, см. недавние работы [P. Boyvalenkov, T. Marinova, M. Stoyanova, Nonexistence of a few binary orthogonal arrays, Discrete Appl. Math. 217 (2) (2017) 144–150. `http://doi.org/10.1016/j.dam.2016.07.023`] и [D. A. Bulutoglu, K. J. Ryan, Integer programming for classifying orthogonal arrays, Australas. J. Comb. 7 (3) (2018) 362–385] и ссылки в них.

3. Подробное описание работы, включая используемые алгоритмы.

Для описания алгоритма нам понадобятся следующие определения. Гиперкуб, или n-куб – граф, вершинами которого являются слова длины n в двоичном алфавите $\{0,1\}$. Две вершины графа смежны (образуют ребро, являются соседями друг другу), если им соответствуют слова, различающиеся ровно в одной позиции, например `10110` и `10010`. Регулярное разбиение 12-куба с параметрами [[2,10],[6,6]] (аналогично, с другими параметрами) – это разбиение множества вершин на два подмножества, код и его дополнение, со следующими свойствами: каждая кодовая вершина имеет ровно 2 кодовых (и 10 некодовых) соседа, каждая некодовая вершина имеет ровно 6 кодовых (и 6 некодовых) соседей. Согласно упомянутым выше результатам Фон-Дер-Флаасса, характеристическая функция такого кода имеет ровно 1536 единиц (в чем нетрудно убедиться при помощи двойного подсчета ребер, соединяющих код и его дополнение) и корреляционную иммунность 7, и наоборот, булева функция от 12 аргументов с данными параметрами соответствует описанным регулярным разбиениям. Алгоритм характеризации регулярных разбиений, разработанный автором проекта, следующий. Без потери общности считаем, что слово из всех нулей $x_0 = 000000000000$ кодовое. Поскольку у него 2 кодовых соседа, мы также без потери общности можем считать, что это $x_1 = 100000000000$ и $x_2 = 010000000000$, другие 10 слов x_3, ..., x_{12} с одной единицей (то есть веса 1) – некодовые. Далее, чтобы выбрать кодовые слова с двумя единицами (то есть веса два), сделаем следующее наблюдение. Каждое из кодовых слов x_1, ... x_12 имеет одного кодового соседа x_0, и для выполнения условия регулярности разбиения словам x_1 и x_2 необходимо "добрать" по одному соседу веса 2, а словам x_3, ..., x_{12} – ровно по 5 соседей веса два. Из этого легко видеть, что выбор кодовых слов веса 2 соответствует решению частного случая задачи о точном покрытии (exact covering) элементов данного множества (в нашем случае, слов веса 1) данными подмножествами (в нашем случае они соответствуют окрестностям слов веса 2), с кратностями, заданными для каждого элемента (на данном этапе, 1 и 5). Эта задача решается при помощи пакета `libexact` П.Каски и О.Поттонена `https://pottonen.kapsi.fi/libexact.html`, который является реализацией классического X-алгоритма с танцующими связями (dancing links) Д.Кнута.

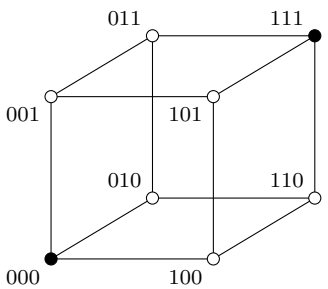
Среди всех найденных решений, нам нужно выбрать неэквивалентные, что делается при помощи сведения к задаче проверки графов на изоморфность (способы такого сведения для проверки эквивалентности кодов описаны в монографии [P. Kaski and P. R. J. Östergård. "Classification Algorithms for Codes and Designs", vol. 15 of Algorithms Comput. Math. Springer, Berlin, 2006. `http://doi.org/10.1007/3-540-28991-7`], где также описаны способы двойного подсчета результатов вычислений, страхующие от вычислительных ошибок), которая решается при помощи пакета `nauty&traces` Б.МакКэя и А.Пиперно, `https://pallini.di.uniroma1.it/`. Далее, алгоритм применяется для восстановления кодовых слов веса 3 всеми возможными неэквивалентными способами, и затем веса 4, после чего регулярное разбиение восстанавливается однозначно, согласно теоретическим результатам. Данного алгоритма, в описанном виде, недостаточно для характеризации всех исследуемых объектов в разумное вычислительное время. Однако удалось разбить множество объектов на подклассы, в соответствии с наличием в регулярном разбиении некоторых подконфигураций, и для каждого из подклассов, в связи с локальными ограничениями, задаваемыми подконфигурациями, описание удалось провести при помощи модификации описанного выше общего алгоритма. Подробнее см. в тексте публикации.

4. Полученные результаты.

Установлено, что существует ровно 103 класса эквивалентности булевых функций от 12 аргументов с 1536 единицами и корреляционной иммунностью 7 (эквивалентно, простых ортогональных массивов $\mathrm{OA}(1536, 12, 2, 7)$, или регулярных разбиений 12-куба с параметрами $[[2, 10], [6, 6]]$), из них ровно две неэквивалентные функции имеют корреляционную иммунность "почти 8", то есть при фиксации 8 переменных число единиц отличается от среднего не более чем на 1. Установлено, что ортогональный массив $\mathrm{OA}(1536, 13, 2, 7)$ единственный с точностью до эквивалентности.

5. Иллюстрации, визуализация результатов.

На иллюстрации показана раскраска вершин 3-куба, соответствующая несбалансированной булевой функцией от 3 аргументов с двумя единицами (отмечены черным цветом), а также регулярному разбиению 3-куба с параметрами $[[0, 3], [1, 2]]$ (черная вершина имеет 0 черных соседей и 3 белых, белая вершина – 1 черного соседа и 2 белых) и ортогональному массиву $\mathrm{OA}(M = 2, n = 3, 2, t = 1)$.



6. Благодарности и публикации

Кластер ИВЦ НГУ помог осуществить исследование, потребовавшее более 20 лет процессорного времени, что неосуществимо на персональных ЭВМ, в разумные сроки.

По результатам вычислительных и теоретических исследований опубликована статья, вторая статья в процессе подготовки (в настоящее время опубликован препринт с описанием вычислительного исследования).

- D. S. Krotov. On the OA(1536,13,2,7) and related orthogonal arrays. Discrete Math. 343(2) 2020, paper 111659, 1-11. `https://doi.org/10.1016/j.disc.2019.111659` (препринт-версия `https://arxiv.org/abs/1905.11371`)
- D. S. Krotov. [[2,10],[6,6]]-equitable partitions of the 12-cube. ArXiv.org preprint, 2020. `https://arxiv.org/abs/2012.00038`