

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И
КИБЕРНЕТИКИ

На правах рукописи

Карелина Екатерина Константиновна

**Методы синтеза
корреляционно-иммунных функций на
основе минимальных функций.**

2.3.6 - Методы и системы защиты информации, информационная
безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
д. ф.-м. н., доцент,
Логачев Олег Алексеевич

Москва - 2024

Оглавление

Введение	5
Глава 1 Основные определения, понятия и обозначения	23
1.1 Основные параметры булевых функций	23
Глава 2 Метод построения минимальных СИ-функций и СИ-функций	33
2.1 Отображения AC^w и DC_i . Описание метода	33
2.2 Свойства отображений AC^w и DC_i	38
2.3 Примеры действия отображений $AC_{v,i}^w$ и DC_i . . .	40
2.4 Критерий равенства получаемых СИ-функций при использовании отображения AC^w	42
2.5 Верхняя оценка мощности множества СИ-функций, получаемых с помощью отображения AC^w	46
2.6 Нижняя оценка мощности множества СИ-функций, получаемых с помощью отображения AC^w	50
2.7 Результаты применения предложенного метода по- строения СИ-функций	57
2.8 Построение классификации минимальных СИ-функций и СИ-функций от 4, 5 и 6 переменных относитель- но группы Джевонса	64

2.8.1	Построение классификации минимальных CI-функций и CI-функций от 4 переменных относительно группы Джевонса	64
2.8.2	Построение классификации минимальных CI-функций и CI-функций от 5 переменных относительно группы Джевонса	66
2.8.3	Построение классификации минимальных CI-функций от 6 переменных относительно группы Джевонса	68

Глава 3 Комбинаторные и спектральные свойства минимальных CI-функций 72

3.1	Достаточное условие существования минимальных CI-функций	72
3.2	Спектральный критерий минимальности CI-функций	74
3.3	Существенные переменные минимальных CI-функций	75
3.4	Весовые свойства минимальных CI-функций . . .	77
3.5	Пример использования минимальных CI-функций для исследования окрестностей заданных CI-функций	80
3.6	Разложения CI-функций на минимальные CI-функции	85
3.6.1	Разложения CI-функций от 4 переменных на минимальные CI-функции	86
3.6.2	Разложения CI-функций от 5 переменных на минимальные CI-функции	87
3.6.3	Разложение функции-константы 1 на минимальные CI-функции	89

Глава 4	Асимптотические оценки мощностей множеств	
	$CI(n, w)$ и $BCI(n, w)$	91
4.1	Оценка мощности множества $CI(n, w)$	91
4.2	Оценка мощности множества $BCI(n, w)$	93
4.3	Верхняя оценка мощности множества $CI(n, w)$. .	97
Заключение		100
Приложение		110
4.4	Классификация CI-функций от 4 переменных . . .	110
4.5	Все минимальные CI-функций от 4 переменных . .	111
4.6	Мощности множеств CI-функций, полученных с помощью отображения $AC_{v,i}^w$	113
4.6.1	Результаты для CI-функций и минималь- ных CI-функций от 4 переменных	113
4.6.2	Результаты для минимальных CI-функций от 5 переменных	119
4.6.3	Результаты для минимальных CI-функций от 6 переменных	122

Введение

Общая характеристика работы. В диссертационной работе приводятся результаты исследования вопросов, связанных с построением корреляционно-иммунных функций (далее, СИ-функций), а также с изучением свойств минимальных СИ-функций. Доказываются некоторые оценки мощности множества СИ-функций от фиксированного числа переменных.

Концепция булевых СИ-функций была предложена Т. Зигенталером (Т. Siegenthaler) в 1985 году. Она явилась итогом осмысления и структуризации семейства методов анализа комбинирующих и фильтрующих генераторов псевдослучайных двоичных последовательностей, называемых корреляционными методами. Реализация корреляционного метода использует существующие в математической модели исследуемого генератора статистические связи между значением комбинирующей (фильтрующей) функции и некоторыми ее переменными. В качестве математического аппарата реализации корреляционного метода использовались, например, статистические процедуры Неймана-Пирсона, позволяющие рассчитывать параметры корреляционного метода, определяющие его эффективность.

В математической модели понятие СИ-функций рассматривает статистическую независимость значения булевой функции от некоторых подмножеств ее переменных, которая снижает эффективность корреляционных методов. Именно такие функции получили название СИ-функций.

Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6 (физико-математические науки) по следующим областям исследования:

1. теория и методология обеспечения информационной безопасности и защиты информации;
5. методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;
10. модели и методы оценки защищенности информации и информационной безопасности объекта;
15. принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности;
19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

В рамках исследования применяется математический аппарат алгебры, булевых функций и комбинаторики, а также вычислительная техника для построения СИ-функций, их классификаций и для подсчета различных параметров рассматриваемых функций.

Актуальность работы. Современное общество трудно представить без использования информационных и телекоммуникационных систем. Стремительное развитие информационных технологий с их быстро растущим потенциалом привело к возможности объединения таких разнородных систем в единые информационно-телекоммуникационные системы. Такие системы стали использоваться повсеместно, и они оказывают все большее влияние на все сферы человеческой деятельности. Информация стала одним из главных и мощных ресурсов государств.

Быстрые темпы научно-технического прогресса в информационной сфере привели к возникновению целого ряда угроз безопасности ИТ-систем со стороны злоумышленников, к числу которых относятся: различные виды мошенничества, компьютерных преступлений, шпионаж, диверсии, несанкционированный доступ и т.п. Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но и оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Таким образом, актуальной становится задача построения защищенных систем, анализ возможных угроз и разработка средств и методов их защиты.

Синтез криптографических примитивов, входящих в состав средств обеспечения информационной безопасности, зачастую использует булевы математические модели и сводится к построению булевой функции или системы булевых функций от достаточно большого числа переменных, обладающих набором определенных свойств. Эти свойства (такие как высокая нелинейность, корреляционная иммунность, алгебраическая иммунность и многие другие) формируются и исследуются в ходе анализа средств обеспечения информационной безопасности. В частности, аппарат булевых функций играет важную роль при построении адекватных математических моделей генераторов псевдослучайных последовательностей и усложняющих преобразований (S-блоков, см. [37]).

С теоретической точки зрения процессы синтеза криптографических примитивов характеризуются следующими факторами. Как известно (см. [18]), почти все функции и системы функций алгебры логики допускают лишь очень сложную реализацию, вследствие

чего фактически недоступны. Кроме того, отсутствуют содержательные (высокие) нижние оценки алгоритмической сложности методов анализа средств обеспечения информационной безопасности, что затрудняет эффективное обоснование сложности задач обращения криптографических функций (примитивов). В силу указанных факторов оценка качеств средств обеспечения информационной безопасности осуществляется в виде экспертного заключения, учитывающего уровень развития методов анализа указанных средств и уровень развития вычислительной техники.

Для построения качественных средств защиты информации при синтезе их математических моделей необходимо использовать булевы функции, обладающие различными наборами свойств, часто являющимися взаимно противоречивыми. Сказанное выше обуславливает важность развития эффективных методов синтеза криптографических булевых функций, позволяющих оптимизировать свойства рассматриваемых булевых функций. Данная работа посвящена синтезу корреляционно-иммунных функций.

В работах Т. Зигенталера [39, 40, 41, 42] были получены основные необходимые и достаточные условия корреляционной иммунности фиксированного порядка (теоретико-информационные, вероятностные, комбинаторные, спектральные). Другие работы посвящены установлению связи понятия СИ-функции фиксированного порядка с некоторыми комбинаторными объектами. Например, с ортогональными таблицами (массивами - см. [25], [32]). Достаточно подробно вопросы синтеза СИ-функций освещены в книгах [17, 26, 29, 44].

Существуют различные подходы к синтезу СИ-функций. Самым простым с идейной точки зрения является переборный метод, в процессе которого проверяются необходимые и достаточные условия кор-

реляционной иммунности для функций, выбираемых из некоторого подходящего множества. Преимуществами данного метода синтеза является его простота и надежность. Кроме того, в ходе реализации перебора как вспомогательный материал могут быть использованы результаты групповых классификаций (относительно группы Джевонса и полной аффинной группы) булевых функций от небольшого числа переменных.

Комбинаторные методы синтеза, рассмотренные в работах [25, 39] (их также можно найти в [44]), в основе своей содержат операцию конкатенации таблиц значений пары булевых функций от n переменных. При этом различные варианты выбора этих функций позволяют построить булеву функцию от $(n+1)$ переменной как с сохранением порядка корреляционной иммунности, которым обладали исходные функции от n переменных, так и с увеличением порядка корреляционной иммунности на единицу.

Некоторые методы синтеза СИ-функций основаны на использовании булевых функций из фиксированных функциональных классов. При этом для обеспечения необходимого уровня корреляционной иммунности используются определенные конструктивные особенности булевых функций из данного фиксированного класса. Приведем два наиболее характерных примера.

Рассмотрим так называемый класс Майорана-Мак-Фарланда булевых функций. Первоначально он стал известен как один из базовых классов для синтеза бент-функций (см. [17, 26]). Неформально конструкцию булевой функции из этого класса можно описать следующим образом. Множество переменных конструируемой булевой функции разбивается на два непересекающихся подмножества мощностей k и m соответственно, $k + m = n$. Конкретную функцию

из класса Майорана-Мак-Фарланда определяет семейство из $k + 1$ -ой булевых функций от m переменных. Первые k из них образуют функцию, отображающую строки длины m битов в строки длиной k битов. Задав верхнюю границу t для минимума весов строк-значений этой функции, мы можем с помощью конструкции Майорана-Мак-Фарланда построить $(t-1)$ -устойчивую булеву функцию (т.е. уравновешенную корреляционно-иммунную порядка $t-1$ булеву функцию).

Второй пример связан с классом так называемых алгебраически вырожденных булевых функций (см., например, [45]). Несмотря на имеющуюся в названии данного класса некоторую «негативную» коннотацию, алгебраически вырожденные булевы функции регулярно используются при синтезе криптографических механизмов. Неформально алгебраически вырожденная функция от n переменных может быть представлена в виде суперпозиции некоторой булевой функции от k переменных, $k < n$, и k линейных булевых функций, множество-объединение существенных переменных которых имеет мощность n . Алгебраически такая функция может быть также представлена в виде композиции линейного отображения, описываемого булевой матрицей размера $k \times n$, и булевой функции от k переменных. Фиксируя те или иные свойства функции от k переменных и $(k \times n)$ -матрицы, мы можем добиваться выполнения определенных свойств у результирующей алгебраически вырожденной булевой функции от n переменных. В частности, если указанная матрица является порождающей матрицей линейного двоичного $[n, k, d]$ -кода, то для любой булевой функции от k переменных порядок корреляционной иммунности результирующей алгебраически вырожденной булевой функции от n переменных не менее $d - 1$ ([44], [45]). Кроме того, использование семейств линейных кодов, исправляющих ошиб-

ки и обладающих некоторыми специальными свойствами, позволяет с использованием данной техники строить семейства СИ-функций.

Активно разрабатывался класс методов синтеза СИ-булевых функций, обладающих рядом дополнительных свойств, называемых рекурсивными методами (в качестве дополнительных свойств фигурировали - нелинейность, алгебраическая иммунность, уравнишенность и т.п.). Суть рекурсивного метода состоит в следующем. Первоначально выбирается СИ-функция от небольшого числа переменных (либо из известного класса, либо полученная методом перебора). Далее с помощью рекурсивных процедур к исходной функции добавляются новые переменные (например, пара переменных), что приводит к появлению булевой функции от большего числа переменных, обладающую необходимыми свойствами. Это рекурсивное преобразование может быть реализовано бесконечное число раз, что порождает бесконечную серию СИ-функций, для которых параметры, задающие дополнительные свойства, удовлетворяют соответствующим асимптотическим соотношениям. Достаточно подробно такие рекурсивные методы синтеза рассмотрены в работах [5], [6], [7], [8], [9], [10], [19], [20].

В качестве еще одного подхода к синтезу СИ-функций в работе [1] было введено понятие минимальной СИ-функции, и было доказано, что любая СИ-функция раскладывается в сумму минимальных СИ-функций с непересекающимися носителями. Данное свойство было предложено использовать для построения СИ-функций: СИ-функция с целевыми параметрами ищется среди функций, построенных с помощью специальным образом подобранного множества минимальных СИ-функций. Однако остается открытым вопрос, как строить сами минимальные СИ-функции.

В дополнение к информации о методах синтеза СИ-функций необходимо упомянуть асимптотическую формулу для числа корреляционно-иммунных порядка k булевых функций, доказанную в работе [11] и имеющую важное методологическое значение для всех направлений исследований по тематике СИ-функций. К сожалению, в этой работе автором была допущена неточность, которую он исправил в работе [12].

В части, касающейся использования понятийного аппарата (терминологической базы), необходимо отметить, что наряду с термином « k -устойчивая функция» (т.е. уравновешенная СИ-функция от n переменных порядка k) используются также и иные термины. В частности, например, в работах, исследующих схемную сложность булевых функций методами гармонического анализа, используют термин « k -сбалансированная n -местная булева функция» (k -balanced Boolean function - см. [22]), что в нашей терминологии означает СИ-функция от n переменных порядка $n - k$.

Цели диссертационной работы заключаются в разработке математического аппарата и новых методов синтеза СИ-функций и минимальных СИ-функций от большого числа переменных, обладающих положительными криптографическими свойствами, а также в исследовании свойств минимальных СИ-функций и получении оценок мощности множеств СИ-функций и минимальных СИ-функций. Для достижения цели были поставлены следующие задачи:

1. разработать математический аппарат и метод построения СИ-функций и минимальных СИ-функций, позволяющий строить СИ-функции от неограниченного числа переменных, используя СИ-функций от малого числа переменных;

2. построить классификацию минимальных СИ-функций от 4, 5, 6 переменных для их использования в качестве «стартовых» функций в предложенном методе;
3. построить с помощью предложенного метода и вычислительной техники устойчивые функции от 7, 8, 9, 10 и 11 переменных;
4. разработать математический аппарат для оценки мощностей множеств СИ-функций и минимальных СИ-функций, получаемых с помощью предложенного метода; провести сравнение теоретических значений мощностей множеств полученных СИ-функций с реальными значениями для СИ-функций от 4, 5 и 6 переменных;
5. изучить свойства множества минимальных СИ-функций, такие как вес минимальных СИ-функций и существенные переменные минимальных СИ-функций; сформулировать и доказать критерий минимальности и достаточное условие минимальности;
6. получить верхнюю оценку мощности множества СИ-функций от n переменных заданного веса.

На защиту выносятся: обоснование актуальности, научная новизна, практическая значимость работы, а также следующие основные положения, которые подтверждаются результатами исследования, представленными в заключении диссертации:

1. Метод построения СИ-функций и минимальных СИ-функций. Критерий равенства СИ-функций, получаемых с помощью данного метода.

2. Классификация относительно группы Джевонса CI-функций и минимальных CI-функций от 4, 5, 6 переменных.
3. Результаты применения предложенного метода и примеры использования минимальных CI-функций для построения устойчивых CI-функций от 7, 8, 9, 10 и 11 переменных.
4. Оценки мощностей множеств CI-функций и минимальных CI-функций, получаемых с помощью данного метода.
5. Свойства минимальных CI-функций: вес функций и их существенные переменные, спектральный критерий минимальности, достаточное условие существования минимальных CI-функций.
6. Асимптотические оценки мощностей множеств $CI(n, w)$ и $BCI(n, w)$, верхняя оценка для мощности множества $CI(n, w)$.

Научная новизна. В диссертации получены следующие новые результаты.

1. Предложено отображение AC^w и на его основе сформулирован метод построения CI-функций и минимальных CI-функций, основанный на комбинации рекурсивного и переборного методов. В работе доказано, что результатом применения отображения AC^w к CI-функции и минимальной CI-функции является CI-функция и минимальная CI-функция соответственно. Данный метод использует известные CI-функции и минимальные CI-функции от малого числа переменных и позволяет строить CI-функции и минимальные CI-функции соответственно уже от большего числа переменных.

2. Получена классификация относительно группы Джевонса минимальных СИ-функций от 4, 5, 6 переменных.
3. Построены устойчивые функции от 7, 8, 9, 10, 11 переменных с помощью предложенного метода.
4. В работе получена оценка мощности получаемых множеств СИ-функций и минимальных СИ-функций с помощью данного метода.
5. Понижена верхняя оценка веса минимальных СИ-функций. Доказано, что любая минимальная СИ-функция существенно зависит от всех своих переменных. Доказан критерий минимальности и сформулировано достаточное условие существования минимальных СИ-функций.
6. Получены асимптотические оценки множеств $CI(n, w)$ и $BCI(n, w)$. Данные оценки используются для доказательства верхней оценки мощности множества $CI(n, w)$.

Практическая значимость. Большая часть результатов диссертации имеет теоретический характер. Полученные результаты могут быть полезны в теории булевых функции, при построении, разработке и анализе потоковых шифров.

Публикации по теме исследования. Результаты работы изложены в 5 публикациях по теме диссертации, 4 из которых опубликованы в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова.

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ

по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность» и входящих в базы цитирования Scopus, Web of Science и RSCI:

- Карелина Е. К. «Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных» / Алексеев Е. К., Карелина Е. К. // Дискретная математика. — 2015. — Т.27, №1. — С.22-33.

DOI: <https://doi.org/10.4213/dm1312> (1.39 п.л. / авторский вклад - 1.39 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506). / Соавтор верифицировал полученные практические результаты. /

Перевод:

Alekseev E. K., Karelina E. K. «Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables» // Discrete Mathematics and Applications. — 2015. — Т.25, №4. — С.193-202. DOI: <https://doi.org/10.1515/dma-2015-0019> (Web of Science, Scopus, SJR — 0.177).

- Karelina E.K., «On construction of correlation-immune functions via minimal functions» / Alekseev E.K., Karelina E.K., Logachev O.A. // Математические вопросы криптографии. — 2018 — Т.9, №2. — С. 7-22 DOI: <https://doi.org/10.4213/mvk251> (1.85 п.л. / авторский вклад - 0.45 п.л. Входит в перечень ВАК РФ, RSCI, ИФ РИНЦ 2022: 0,548). / Соавторам принадлежит формулирование метода построения СИ-функций, основанного на переборе СИ-функций в некотором подпространстве. Базис для этого пространства может быть построен с помощью метода, предложен-

ного автором настоящей диссертации (раздел 4.1 по тексту статьи). Также Карелиной Е. К. получены практические результаты использования предложенного метода (раздел 6 по тексту)./

- Карелина Е. К. «Об одном методе синтеза корреляционно-иммунных булевых функций» // Дискретная математика. — 2018. — Т.30, №4. — С.12-28 DOI: <https://doi.org/10.4213/dm1524> (1.96 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506).

Перевод:

Karelina E. K. «On a method of synthesis of correlation-immune Boolean functions» // Discrete Mathematics and Applications. — 2020. — Т.30, №2. — С.79-91. DOI: <https://doi.org/10.1515/dma-2020-0008> (Web of Science, Scopus, SJR — 0.177).

- Карелина Е. К. «Мощностные оценки множества корреляционно-иммунных булевых функций» // Дискретная математика. — 2021. — Т.33, №1. — С.12-19 DOI: <https://doi.org/10.4213/dm1628> (0.92 п.л. Входит в перечень ВАК РФ, RSCI, двухлетний ИФ РИНЦ 2022: 0,506).

Перевод:

Karelina E. K. «Some cardinality estimates for the set of correlation-immune Boolean functions» // Discrete Mathematics and Applications. — 2022. — Т.32, №2. — С. 91-96. DOI: <https://doi.org/10.1515/dma-2022-0008> (Web of Science, Scopus, SJR — 0.177).

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

- Карелина Е. К. «Мощностные оценки множества корреляционно-иммунных функций, получаемого с помощью отображения AC^w ,» // International Journal of Open Information Technologies. — 2022. — Т.10, №1. — С. 28-35 (0.92 п.л. Двухлетний ИФ РИНЦ 2023: 0,842).

Апробация работы. Результаты, представленные в диссертации, докладывались на следующих международных и отечественных научных конференциях и семинарах:

- на семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета Вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова, неоднократно в 2014-2015 годах;
- на семинаре отдела математических проблем информационной безопасности ИПИБ МГУ имени М. В. Ломоносова, неоднократно в 2015-2017 годах;
- на семинаре «Булевы функции в криптологии» кафедры дискретной математики Механико-математического факультета Московского государственного университета имени М. В. Ломоносова, неоднократно в 2013-2015 годах;
- на VI международной научной конференции «Современные тенденции в криптографии», г. Санкт-Петербург, 5-7 июня в 2017 году.

Структура и объем работы

Диссертационная работа состоит из введения, одного вспомога-

ного раздела, трех глав, заключения, списка литературы из 45 наименований и приложения. Работа изложена на 125 страницах.

Содержание работы

Во **Введении** обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В **первой главе** диссертации приводятся основные понятия и ранее известные результаты, которые используются далее в работе или представляются важными для понимания следующих глав.

Во **второй главе** описывается метод построения минимальных СИ-функций, основанный на комбинации переборного и рекурсивного методов. В части, касающейся перебора, строятся минимальные СИ-функции от малого числа переменных. Такие функции можно получить с помощью вычислительной техники (примеры функций приведены в данной работе и в работах [4], [13]). Далее рекурсивно, используя известные минимальные СИ-функции от малого числа переменных, строятся минимальные СИ-функции от большего числа переменных. Метод прост в реализации и позволяет быстро наращивать число переменных. Предложенный метод позволяет реализовать указанный выше альтернативный подход: сначала рекурсивно строятся подходящие минимальные СИ-функции от нужного числа переменных («опорные точки»), которые затем используются для поиска функций с нужными параметрами без изменения количества переменных. Другие возможности использования минимальных СИ-функций для решения задач построения булевых функций можно найти в работе [21].

В основе предложенного рекурсивного метода для наращивания

числа переменных лежит использование отображения AC^w . Данное отображение вводится в разделе 2.1. Также в этом разделе вводится отображение DC_i . Действие этого отображения является обратным к действию отображения AC^w : отображение DC_i позволяет уменьшать число переменных. Доказывается, что применение данных отображений к уже известной CI-функции (минимальной CI-функции) с определенными значениями параметров отображений позволяет строить CI-функции (минимальные CI-функции соответственно) от большего или меньшего числа переменных. В этом же разделе описывается сам процесс построения CI-функций.

В следующем разделе 2.2 доказываются некоторые свойства введенных отображений. В разделе 2.3 приводятся примеры действий отображений к заданным функциям.

Применение отображения $AC_{v,i}^w$ к одной и той же функции со всеми возможными параметрами позволяет получить в том числе и равные между собой функции. В разделе 2.4 приводится критерий равенства двух функций, которые получаются при применении отображения $AC_{v,i}^w$ к некоторой заданной начальной функции. Данный критерий используется при доказательстве нижней и верхней оценок мощности множества CI-функций, которое получается при применении данного отображения к исходной CI-функции. Значение верхней оценки приведено в разделе 2.5, значение нижней оценки — в разделе 2.6.

Рекурсия в процессе построения минимальных функций от большого числа переменных приводит к необходимости исследования «опорных точек» — минимальных CI-функций от малого числа переменных, в том числе создания их классификации относительно групп, которые сохраняют определенный набор их свойств. Построе-

ние классификаций является эффективным и широко применяемым методом исследования свойств и компактного перечисления булевых функций. Примеры классификаций можно найти в работах [4], [13], [23], [24], [33], [31].

В разделе 2.7 приводятся результаты применения предложенного метода построения функций.

Раздел 2.8 посвящен построению классификации минимальных СИ-функций и СИ-функций от малого числа переменных относительно группы Джевонса. В разделе 2.8.1 приведена классификация минимальных СИ-функций и СИ-функций от 4 переменных, в разделе 2.8.2 приведена классификация минимальных СИ-функций и СИ-функций от 5 переменных, в разделе 2.8.3 приведена классификация минимальных СИ-функций от 6 переменных.

Третья глава посвящена изучению некоторых свойств минимальных СИ-функций.

В разделе 3.1 доказывается достаточное условие существования минимальных СИ-функций. При доказательстве используется свойство отображения $AC_{v,i}^w$. Доказывается, что для любого $n \geq 5$ существуют минимальные СИ-функции веса 6 и веса 8, а для любого $n \geq 6$ существуют минимальные СИ-функции веса 10.

В разделе 3.2 приводится критерий минимальности СИ-функции, основанный на исследовании спектра исходной СИ-функции (коэффициентов Уолша).

В разделе 3.3 доказывается теорема о существенных переменных минимальных СИ-функций. Доказанная теорема показывает, что минимальную СИ-функцию от n переменных нельзя описать с помощью минимальной СИ-функции от $n - 1$ переменной, так как минимальная СИ-функция существенно зависит от всех своих переменных.

В разделе 3.4 уточнена верхняя оценка веса минимальных СИ-функций. В работе [1] было доказано, что вес минимальных СИ-функций меньше 2^{n-1} для $n \geq 4$. В данной работе оценка понижена до $2^{n-1} - 2$ для $n \geq 4$.

В работе [21] было предложено использовать минимальные СИ-функции для исследования «окрестностей» заданных СИ-функций. Для этого требуется разложить заданную СИ-функцию на минимальные СИ-функции. Результат использования предложенного подхода можно найти в разделе 3.5. В разделе 3.6 приведены некоторые характеристики разложений СИ-функций, а также характеристики разложения константы **1** на минимальные СИ-функции от 4 и 5 переменных.

В **четвертой главе** исследуются вопросы оценок мощности множества СИ-функций. В работе [1], посвященной изучению свойств СИ-функций, рассматривалось строение множества СИ-функций. Автором было введено множество $BCI(n, w)$, и было доказано, что подсчет мощности множества СИ-функций от n переменных сводится к подсчету мощности множества $BCI(n, w)$ для каждого $w = 0, \dots, 2^{n-1}$.

В разделе 4.1 приводится асимптотическая оценка мощности СИ-функций фиксированного веса, в разделе 4.2 асимптотическая оценка мощности множества $BCI(n, w)$. Верхняя оценка мощности множества $CI(n, w)$ доказывается в разделе 4.3. В работе проводится сравнение полученных оценок с точными значениями, вычисленными теоретически или с помощью вычислительной техники.

В **Заключении** перечислены основные результаты диссертации. В **Приложении** содержатся таблицы с практическими результатами.

Глава 1

Основные определения, понятия и обозначения

В данной главе вводятся основные определения, понятия и ранее известные результаты, необходимые для понимания последующих глав диссертации. Также вводятся обозначения, которые будут использоваться в дальнейшем.

1.1 Основные параметры булевых функций

В данном разделе даются определения и результаты, имеющие важное значение при изучении булевых функций.

Пусть $\mathbb{F}_2$ — конечное поле из двух элементов, операции сложения и умножения в котором вводятся как обычные операции сложения и умножения чисел 0 и 1 по модулю 2. Для произвольного натурального числа n обозначим через $V_n = \mathbb{F}_2^n$ векторное пространство наборов длины n с компонентами из поля $\mathbb{F}_2$. Пусть $V_n^* = V_n \setminus \{0^n\}$, где $0^n = (\underbrace{0, \dots, 0}_n) \in V_n$.

Будем обозначать через $u^{(i)}$ — i -ую координату вектора $u \in V_n$. *Весом* вектора $u \in V_n$ называется число единиц в u .

Множество всех булевых функций от n переменных $f : V_n \rightarrow \mathbb{F}_2$ будем обозначать $\mathcal{F}_n$. Константные булевы функции обозначим через **1** и **0**. Для булевой функции $f \in \mathcal{F}_n$ *носителем* называют множества вида $\text{supp}(f) = \{x \in V_n \mid f(x) = 1\}$, а мощность данного множества — *весом* булевой функции $wt(f)$. Для функции $f \in \mathcal{F}_n$ *таблицей*

истинности называется $(wt(f) \times n)$ -матрица, строками которой являются строки из носителя функции. Считаем, что в такой матрице все строки лексикографически упорядочены сверху вниз. Для пары булевых функций $f, g \in \mathcal{F}_n$ расстояние Хэмминга $dist(f, g)$ определяют как мощность множества $\{x \in V_n \mid f(x) \neq g(x)\}$. Алгебраическую степень полинома Жегалкина булевой функции $f \in \mathcal{F}_n$ будем обозначать как $deg(f)$. Обозначим множество $\mathcal{A}_n = \{f \in \mathcal{F}_n \mid deg(f) \leq 1\}$. Такие функции называются *аффинными*.

Определение 1. *Преобразование Уолша-Адамара* булевой функции $f \in \mathcal{F}_n$ называют целочисленную функцию на V_n , которая определяется равенством

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle x, u \rangle}$$

(суммирование производится в действительной области).

Для каждого $u \in V_n$ значение $W_f(u)$ называют коэффициентом Уолша-Адамара булевой функции f , соответствующим вектору u .

Определение 2. *Нелинейностью* $nl(f)$ булевой функции $f \in \mathcal{F}_n$ называют расстояние Хэмминга до множества всех аффинных функций:

$$nl(f) = dist(f, \mathcal{A}_n).$$

Значение нелинейности можно вычислить по формуле:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} |W_f(u)|.$$

Для булевой функции $f \in \mathcal{F}_n$ и произвольного вектора $u \in V_n$ будем обозначать через f^u функцию $f^u : x \rightarrow f(x \oplus u)$.

Определение 3. Производной функции $f \in \mathcal{F}_n$ по направлению $u \in V_n^*$ называется функция $D_u f = f^u \oplus f$.

Подфункцией булевой функции f называется функция f' , полученная подстановкой в f констант 0 или 1 вместо некоторых переменных. Если $f \in \mathcal{F}_n$ и вместо переменных $x_{i_1}, x_{i_2}, \dots, x_{i_k}$ подставляются константы $\sigma_1, \sigma_2, \dots, \sigma_k, k \leq n$, соответственно, то полученная подфункция обозначается как $f_{x_{i_1}, x_{i_2}, \dots, x_{i_k}}^{\sigma_1, \sigma_2, \dots, \sigma_k} \in \mathcal{F}_{n-k}$.

Определение 4. Пространством линейных структур функции $f \in \mathcal{F}_n$ называется множество $L_f = \{u \in V_n^* \mid D_u f = \text{const}\}$. Все u , входящие в это множество, называются *нетривиальными линейными структурами* функции f .

Множество булевых функций $f \in \mathcal{F}_n$, имеющих нетривиальные линейные структуры, обозначается через $\mathcal{F}_n^0$.

Пусть A — $(n \times k)$ -матрица над $\mathbb{F}_2$, а f — булева функция от k переменных. Через f^A будем обозначать функцию от n переменных, определенную следующим образом: $f^A : x \rightarrow f(xA)$.

Определение 5. Порядком алгебраической вырожденности $AD(f)$ булевой функции $f \in \mathcal{F}_n$ называется максимально возможное значение $n - k$, где целое число $0 \leq k \leq n$ таково, что существуют такие функция $g \in \mathcal{F}_k$ и $(n \times k)$ -матрица D над $\mathbb{F}_2$, что выполнено равенство $f = g^D$.

Определение 6. Функции, для которых $AD(f) > 0$, называются *алгебраически вырожденными*.

Множество всех алгебраически вырожденных функций от n переменных обозначим через $DG(n) = \{f \in \mathcal{F}_n \mid AD(f) > 0\}$.

Определение 7. *Невырожденностью* функции $f \in \mathcal{F}_n$ называется значение

$$\rho(f) = \text{dist}(f, DG(n)).$$

В работе [35] была введена следующая мера нелинейности для функции $f \in \mathcal{F}_n$:

$$\delta(f) = \text{dist}(f, \mathcal{F}_n^0).$$

Определение 8. Булева функция $f \in \mathcal{F}_n$ называется *корреляционно-иммунной порядка c* , $0 < c \leq n$, если выход f и любое множество из c ее входных переменных являются статистически независимыми [39]. В эквивалентной формулировке булеву функцию $f \in \mathcal{F}_n$ называют *корреляционно-иммунной порядка c* , $0 < c \leq n$, если для любой ее подфункции f' от $n - c$ переменных выполнено равенство:

$$\text{wt}(f') = \frac{\text{wt}(f)}{2^c}$$

[19]. Из определения следует, что все корреляционно-иммунные функции имеют четный вес.

Корреляционно-иммунная функция порядка c является корреляционно-иммунной любого меньшего порядка, поэтому удобно использовать обозначение

$$\text{cor}(f) = \max\{c \in \mathbb{N} \mid f \text{ — корреляционно-иммунна порядка } c\}.$$

Обозначим множество всех корреляционно-иммунных булевых функций как минимум первого порядка, зависящих от n переменных, через $CI(n)$.

Определение 9. Функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $wt(f) = 2^{n-1}$. Уравновешенная корреляционно-иммунная булева функция $f \in \mathcal{F}_n$ порядка s называется *s -устойчивой*.

Справедлив следующий критерий корреляционной иммунности.

Теорема 1. [39] Булева функция $f \in \mathcal{F}_n$ корреляционно-иммунна порядка s тогда и только тогда, когда для любого вектора $u \in V_n$ такого, что $1 \leq wt(f) \leq s$, выполнено равенство $W_f(u) = 0$.

Определение 10. Ортогональным массивом размера $m \times n$ с ограничениями уровня 2, силы t и индекса ν называют $(m \times n)$ -матрицу M над полем $\mathbb{F}_2$, обладающую свойством: в любом подмножестве из t столбцов матрицы M любой из 2^t векторов пространства V_t встречается как строка ровно ν раз (см. [20]). Обозначается $OA_\nu(m, n, 2, t)$.

Теорема 2. [25] Для любой функции $f \in \mathcal{F}_n$ выполнено неравенство $cor(f) \geq s$ тогда и только тогда, когда ее таблица истинности является ортогональным массивом $OA_\nu(wt(f), n, 2, s)$.

Для удобства дальнейшего изложения сформулируем простое следствие из Теоремы 2:

Следствие 1. Множество наборов является носителем СИ-функции порядка s тогда и только тогда, когда эти наборы различны, и в таблице, составленной из этих наборов, для любых s столбцов любой вектор из V_s встречается как строка ровно $\frac{wt(f)}{2^s}$ раз.

Очевидно, что в такой таблице все столбцы уравновешенны.

Напомним основное для данной работы понятие минимальной СИ-функции, введенное в работе [1].

Определение 11. Функция $f \in CI(n)$ называется *минимальной корреляционно-иммунной* функцией, если не существует корреляционно-иммунной функции $g \in CI(n)$, для которой выполняется $\text{supp}(g) \subset \text{supp}(f)$.

Известны следующие свойства минимальных CI-функций, доказанные в [1].

Теорема 3. [1] Функция $f \in CI(n)$ является минимальной CI-функцией тогда и только тогда, когда f невозможно разложить в сумму двух CI-функций с непересекающимися носителями (т.е. f нельзя представить в виде суммы $f = g \oplus h$, где $g, h \in CI(n)$ и $h \cdot g = 0$).

Теорема 4. [1] Для любой минимальной CI-функции f выполнено неравенство $\text{wt}(f) < 2^{n-1}$, где $n \geq 4$.

Теорема 5. [1] Для любой минимальной CI-функции f справедливо неравенство $\text{cor}(f) \leq 2$.

Теорема 6. [1] Любая функция $f \in CI(n)$ может быть разложена в сумму минимальных CI-функций с попарно непересекающимися носителями.

Таким образом, зная всё множество минимальных CI-функций от n переменных, можно построить всё множество $CI(n)$, рассматривая всевозможные суммы минимальных CI-функций с попарно непересекающимися носителями.

Множество всех минимальных CI-функций от n переменных обозначается через $MCI(n)$.

Пусть G — группа, состоящая из преобразований множества V_n , и $\mathfrak{g} \in G$. Через $f^{\mathfrak{g}}$ обозначим следующую функцию: $f^{\mathfrak{g}}(x) = f(\mathfrak{g}(x))$. Через f^G обозначим множество $f^G = \{f^{\mathfrak{g}} \mid \mathfrak{g} \in G\}$.

Рассмотрим отношение эквивалентности на множестве функций:

$$f \sim h \Leftrightarrow \exists \mathfrak{g} \in G : f^{\mathfrak{g}} = h.$$

Множество f^G — класс эквивалентности, представителем которого является функция f .

Под классификацией некоторого множества M булевых функций относительно некоторой группы G понимается множество всех различных классов эквивалентности f^G , где $f \in M$. Для задания некоторого класса эквивалентности далее будем приводить какого-либо его представителя.

Определение 12. Группой Джевонса $\mathcal{D}_n$ называют группу, состоящую из $2^n \cdot n!$ перестановок вида

$$\mathfrak{g} : (x_1, \dots, x_n) \mapsto (x_{j_1} \oplus a_1, \dots, x_{j_n} \oplus a_n),$$

где $\begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix}$ — перестановка на множестве $\{1, \dots, n\}$ и

$$a = (a_1, \dots, a_n) \in V_n.$$

Для элементов группы $\mathcal{D}_n$ справедливо следующее утверждение.

Теорема 7. [17] Для любой CI-функции (минимальной CI-функции) $f \in \mathcal{F}_n$ порядка s , $0 < s \leq n$, и элемента $\mathfrak{g} \in \mathcal{D}_n$ функция $f^{\mathfrak{g}} \in \mathcal{F}_n$ также является CI-функцией (минимальной CI-функцией) порядка s .

Обозначим через $CI^w(n)$ и $CI_c(n)$ множество всех СИ-функций от n переменных, в котором любая функция имеет вес w , где w — четное число, и множество всех СИ-функций от n переменных, в котором любая функция имеет порядок корреляционной иммунности равный c , соответственно. Через $CI_c^w(n)$ обозначим множество всех СИ-функций от n переменных, в котором любая функция имеет вес w , где w — четное число, и порядок корреляционной иммунности равный c .

Обозначим через $\widehat{CI}(n)$ множество классов эквивалентности СИ-функций от n переменных относительно группы Джевонса. Для удобства представления обозначим через $\widehat{CI}^w(n)$ и $\widehat{CI}_c(n)$ множество классов эквивалентности, в котором любая функция имеет вес w , и множество классов эквивалентности, в котором любая функция имеет порядок корреляционной иммунности равный c , соответственно. Через $\widehat{CI}_c^w(n)$ обозначим множество классов эквивалентности, в котором любая функция имеет вес w и порядок корреляционной иммунности равный c .

Аналогичным образом вводятся обозначения для множества $MCI(n)$.

В работе [1] были введены следующие множества.

Определение 13. Через $Mir(n)$ обозначим множество четных булевых функций от $n \in \mathbb{N}$ переменных, то есть таких функций $f \in \mathcal{F}_n$, для которых равенство $f(x) = f(x \oplus 1^n)$ выполнено для любого $x \in V_n$.

Определение 14. Ядром четности функции $f \in \mathcal{F}_n$ называется функция $kt(f) = f \cdot f^{1^n}$.

Определение 15. Через $Anmir(n)$ обозначим множество

$$Anmir(n) = \{f \in \mathcal{F}_n | km(f) = \bar{0}\}.$$

Определение 16. Через $BCI(n)$ обозначим множество

$$BCI(n) = Anmir(n) \cap CI(n).$$

Известны следующие оценки мощности множеств $CI(n)$ и $BCI(n, 4w)$, доказанные в [1].

Утверждение 1. [1] Для мощности CI -функций справедливо равенство:

$$|CI(n)| = \sum_{g \in BCI(n)} 2^{2^{n-1}-wt(g)} = \sum_{w=0}^{2^{n-1}} 2^{2^{n-1}-w} \cdot |BCI(n, w)|.$$

Утверждение 2. [1] Для мощности множества $BCI(n, 4w)$, где $w > 1$, справедливо неравенство:

$$|BCI(n, 4w)| \geq \binom{2^{n-2}}{2w} \cdot \binom{2w}{w}.$$

Утверждение 3. [1] Для мощности множества $CI(n)$ справедливо неравенство:

$$|CI(n)| \geq \sum_{m=0}^{2^{n-3}} 2^{2^{n-1}-4m} \cdot \binom{2^{n-2}}{2m} \cdot \binom{2m}{m}.$$

Также в работе [1] рассматривались функции из множества $BCI(n, 4)$. Все функции из этого множества являются минимальны-

ми СИ-функциями веса 4 от n переменных. В работе доказана формула вычисления мощности множества $BCI(n, 4)$:

Теорема 8. [1]

$$|BCI(n, 4)| = 2^{n-3} \cdot (3^{n-1} - 2^n + 1).$$

В данной работе представлены асимптотические оценки мощностей множеств $CI(n, w)$ и $BCI(n, w)$.

Введем обозначение конкатенации векторов значений функций через $||$: запись $f_1||f_2$ будет означать, что сначала записывается вектор значений функции f_1 , а затем вектор значений функции f_2 .

Везде ниже для описания булевой функции приводится ее запись в сокращенной форме — для вектора значений булевой функции в двоичном представлении четверки подряд стоящих двоичных символов представлены в виде числа в шестнадцатеричной системе счисления. Так, например, сокращенная запись булевой функции $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2 \oplus x_3x_2 \oplus x_1x_3 \oplus x_1x_2x_3$ от 3-х переменных такова:

$$f(x_1, x_2, x_3) = 00110001 = 0x31.$$

Глава 2

Метод построения минимальных СИ-функций и СИ-функций

2.1 Отображения AC^w и DC_i . Описание метода

Приводимые ниже результаты позволяют строить СИ-функции от большего или меньшего числа переменных, используя уже известные СИ-функции. Везде далее будем считать, что все наборы из носителя функции лексикографически упорядочены.

Введем множество $\mathcal{F}_n^w = \{f \in \mathcal{F}_n \mid wt(f) = w\}$. Введем следующие отображения и опишем действия этих отображений на функции:

$$AC^{(w)} : \mathcal{F}_n^w \times V_w \times \{1, \dots, n+1\} \mapsto \mathcal{F}_{n+1}^w.$$

$$AC_{v,i}^w(f) = AC^{(w)}(f, v, i) = g, \text{ где } v = (v^{(1)}, v^{(2)}, \dots, v^{(w)})$$

$$supp(f) = \begin{cases} (u_1^{(1)}, u_1^{(2)}, \dots, u_1^{(i-1)}, u_1^{(i)}, u_1^{(i+1)}, \dots, u_1^{(n)}) \\ (u_2^{(1)}, u_2^{(2)}, \dots, u_2^{(i-1)}, u_2^{(i)}, u_2^{(i+1)}, \dots, u_2^{(n)}) \\ \dots \\ (u_w^{(1)}, u_w^{(2)}, \dots, u_w^{(i-1)}, u_w^{(i)}, u_w^{(i+1)}, \dots, u_w^{(n)}) \end{cases}$$

$$supp(g) = \begin{cases} (u_1^{(1)}, u_1^{(2)}, \dots, u_1^{(i-1)}, v^{(1)}, u_1^{(i)}, u_1^{(i+1)}, \dots, u_1^{(n)}) \\ (u_2^{(1)}, u_2^{(2)}, \dots, u_2^{(i-1)}, v^{(2)}, u_2^{(i)}, u_2^{(i+1)}, \dots, u_2^{(n)}) \\ \dots \\ (u_w^{(1)}, u_w^{(2)}, \dots, u_w^{(i-1)}, v^{(w)}, u_w^{(i)}, u_w^{(i+1)}, \dots, u_w^{(n)}) \end{cases}$$

Поясним, что в случае $i = n + 1$, носитель построенной функции будет иметь следующий вид:

$$supp(g) = \begin{cases} (u_1^{(1)}, u_1^{(2)}, \dots, u_1^{(n)}, v^{(1)}) \\ (u_2^{(1)}, u_2^{(2)}, \dots, u_2^{(n)}, v^{(2)}) \\ \dots \\ (u_w^{(1)}, u_w^{(2)}, \dots, u_w^{(n)}, v^{(w)}). \end{cases}$$

Действие отображения $AC^{(w)}$ заключается в добавлении столбца длины w к таблице истинности функции.

Также опишем следующее отображение. Пусть функция $f \in \mathcal{F}_n$ задана следующим образом:

$$supp(f) = \begin{cases} (u_1^{(1)}, u_1^{(2)}, \dots, u_1^{(i-1)}, u_1^{(i)}, u_1^{(i+1)}, \dots, u_1^{(n)}) \\ (u_2^{(1)}, u_2^{(2)}, \dots, u_2^{(i-1)}, u_2^{(i)}, u_2^{(i+1)}, \dots, u_2^{(n)}) \\ \dots \\ (u_w^{(1)}, u_w^{(2)}, \dots, u_w^{(i-1)}, u_w^{(i)}, u_w^{(i+1)}, \dots, u_w^{(n)}) \end{cases}$$

Если после удаления i -го столбца в таблице истинности нет

одинаковых строк, то полученная таблица

$$\begin{array}{c}
(u_1^{(1)}, u_1^{(2)}, \dots, u_1^{(i-1)}, u_1^{(i+1)}, \dots, u_1^{(n)}) \\
(u_2^{(1)}, u_2^{(2)}, \dots, u_2^{(i-1)}, u_2^{(i+1)}, \dots, u_2^{(n)}) \\
\vdots \\
(u_w^{(1)}, u_w^{(2)}, \dots, u_w^{(i-1)}, u_w^{(i+1)}, \dots, u_w^{(n)})
\end{array}$$

определяет некоторую функцию $g \in \mathcal{F}_{n-1}$, и в этом случае будем полагать $DC_i(f) = g$. Иначе считаем, что $DC_i(f) = \Lambda$. Символ Λ обозначает то, что результат отображения не принадлежит $\mathcal{F}_{n-1}$.

Действие этого отображения заключается в удалении i -го столбца в таблице истинности.

С помощью этих отображений можно строить CI-функции от большего или меньшего числа переменных, используя уже известные CI-функции. Справедливы следующие теоремы:

Предложение 1. Если $f \in CI(n)$ и $w = wt(f)$, то $AC_{v,i}^{(w)}(f) \in CI(n+1)$, для любого v такого, что $wt(v) = \frac{w}{2}$, для любого $i \in \{1, \dots, n+1\}$.

Доказательство. Так как функция f является CI-функцией, то ее таблица истинности состоит из уравновешенных столбцов (см. Следствие 1). Приписывание в эту таблицу уравновешенного столбца сохраняет свойство уравновешенности столбцов в таблице истинности. Значит функция $AC_{v,i}^{(w)}(f)$ является CI-функцией. $\square$

Предложение 2. Если значение $DC_i(f)$ не равно Λ и $cor(f) = c$, то $cor(DC_i(f)) \geq c$, для любого $i \in \{1, \dots, n\}$.

Доказательство. Пусть значение $DC_i(f)$ не равно Λ .

Тогда $cor(DC_i(f)) \geq c$, для любого $i \in \{1, \dots, n\}$, так как после удаления столбца количество столбцов, для которых выполняется Следствие 1, может только увеличиться. $\square$

Для дальнейшего важно, что утверждение, аналогичное Предложению 1, остается справедливым для класса минимальных CI-функций.

Предложение 3. *Если $f \in MCI(n)$ и $w = wt(f)$, то $AC_{v,i}^w(f) = g \in MCI(n+1)$, для любого v такого, что $wt(v) = \frac{w}{2}$, для любого $i \in \{1, \dots, n+1\}$.*

Доказательство. Пусть $f \in MCI(n)$, $AC_{v,i}^w(f) = g$, $wt(v) = \frac{w}{2}$. Покажем, что $g \in MCI(n+1)$.

Предположим, что это не так, то есть $g \notin MCI(n+1)$. В силу Предложения 1 $g \in CI(n+1)$. Тогда из носителя функции g можно выделить подмножество, которое будет являться носителем минимальной CI-функции h , то есть $supp(h) \subset supp(g)$. Это следует из Теоремы 6. Применим к функции h отображение $DC_i : h' = DC_i(h)$. По утверждению Предложения 2 $h' \in CI(n)$. При этом $supp(h') \subset supp(f)$. Получаем противоречие условию, так как в этом случае $f \notin MCI(n)$. $\square$

Таким образом, используя известные минимальные CI-функции и CI-функции от 4, 5 и 6 переменных (примеры таких функций можно найти в работе [4] и в Главе 2.8 настоящей работы), можно построить минимальные CI-функции и CI-функции функции от большего числа переменных.

Сам процесс построения можно разделить на два этапа:

1. выделение множества СИ-функций (минимальных СИ-функций) от малого числа переменных
2. наращивание числа переменных, путем добавления уравновешенных столбцов в таблицу истинности рассматриваемых функций и построение итогового множества СИ-функций (минимальных СИ-функций) от большого числа переменных

Отметим, что итоговое множество не содержит все СИ-функции (минимальные СИ-функции) от полученного числа переменных. Действительно, при увеличении числа переменных растет и возможный вес СИ-функций. Однако применение отображения к известным функциям от меньшего числа переменных сохраняет вес исходной функции. Кроме того, среди функций построенного множества могут быть совпадающие между собой функции.

Для упрощения вычислений и построения множества СИ-функций или множества минимальных СИ-функций отметим следующий факт. Можно добавлять уравновешенный столбец к таблице истинности исходной СИ-функции (минимальной СИ-функции) от n переменных всегда на одну и ту же позицию, например, в конец, ставя его самым последним. Далее применяем всевозможные перестановки переменных к каждой построенной СИ-функции (минимальной СИ-функции) от $n + 1$ переменной. Данный способ построения СИ-функций будет аналогичен способу построения СИ-функций (минимальных СИ-функций) от $n + 1$ переменной, в котором будут добавляться всевозможные уравновешенные столбцы на все позиции таблицы истинности исходных СИ-функции (минимальной СИ-функции) от n переменных.

Результаты применения предложенного метода построения СИ-

функций можно найти в разделе 2.7.

2.2 Свойства отображений AC^w и DC_i

Докажем следующие утверждения о свойствах отображений $AC_{v,i}^w$ и DC_i .

Отметим, что для совершенной ДНФ функции применение отображения $AC^{(w)}$ (DC_i) равносильно приписыванию (вычеркиванию) к каждому конъюнкту переменной x_i или ее отрицания $\bar{x}_i$ одинаковое число раз.

Предложение 4. *Справедливы следующие утверждения:*

- Пусть $w = wt(f)$ и $g = AC_{v,i}^w(f)$. Тогда если $deg(f) = d$, то $deg(g) > d$.
- Пусть $w = wt(f)$ и $DC_i(f) = g$ (считаем, что результат отображения не равен Λ). Тогда если $deg(f) = d$, то $deg(g) < d$.

Доказательство. Докажем первое утверждение. Пусть функция f записана в совершенной ДНФ в следующем виде: $f = K_1 \vee \dots \vee K_w$, где $w = wt(f)$. Применим отображение $AC_{v,i}^w$ к функции f . Получим функцию $g = AC_{v,i}^w(f)$. Как пояснялось выше, к каждому конъюнкту приписется или переменная x_i , или ее отрицание $\bar{x}_i$ (одинаковое число раз при уравновешенном столбце). Обозначим переменную x_i через y . Упорядочим конъюнкты в ДНФ функции g так, чтобы сначала были записаны те конъюнкты, где переменная y без отрицания, затем те конъюнкты, где переменная y с отрицанием. Тогда ДНФ функции g имеет следующий вид: $g = K_1y \vee \dots \vee K_ly \vee K_{l+1}\bar{y} \vee$

$\dots \vee K_w \bar{y}$, где $l = w/2$. Приведем к АНФ. Знак $\vee$ можно заменить на $\oplus$, так как в ДНФ записаны те мономы, на которых функция принимает значение 1. Запишем все переменные y с отрицанием следующим образом: $\bar{y} = y \oplus 1$ и вынесем переменную y за скобки. Тогда в скобках останутся только те мономы, которые в точности определяют функцию f , степень АНФ которой по условию равна d . Запишем все оставшиеся переменные с отрицанием аналогичным образом: $\bar{x} = x \oplus 1$. Раскроем скобки и приведем подобные слагаемые. Получим

$$g = yANF_f \oplus [M_{p+1} \oplus \dots \oplus M_s],$$

где M_i — мономы некоторой степени, ANF_f — АНФ функции f . Понятно, что степень g не меньше $d + 1$. Вместе с тем степень мономов, стоящих в скобках, с учетом раскрытия скобок и приведения подобных слагаемых может превосходить $d + 1$, поэтому окончательно имеем:

$$\deg(g) = \max\{\deg(yANF_f), \max\{\deg(M_{p+1}), \dots, \deg(M_s)\}\} > d.$$

Второе утверждение следует из того, что $\deg(AC_{v,i}^{(w)}(g)) > \deg(f)$, где v — столбец, который был удален после применения отображения DC_i к функции f . $\square$

Предложение 5. Пусть $\text{supp}(f) = (u_1, \dots, u_w)$ и значение отображения $DC_i(f)$ не равно Λ , тогда $AC_{v,i}^w(DC_i(f)) = f$, где $v = (u_1^{(i)}, \dots, u_w^{(i)})$.

Доказательство. Для доказательства этого утверждения достаточно заметить, что сначала из таблицы истинности удаляется столбец, потом он же и приписывается на то же место. $\square$

2.3 Примеры действия отображений $AC_{v,i}^w$ и DC_i

На примере рассмотрим, как действуют эти отображения. Рассмотрим СИ-функцию $f(x_1, x_2, x_3, x_4) = 0x8124$ от 4-х переменных. Ее таблица истинности такова:

0000

0111

1010

1101.

Применим к этой функции отображение $AC_{v,5}^{(4)}$, где $v = (1010)$, $wt(v) = \frac{wt(f)}{2}$. Получим СИ-функцию g от 5-ти переменных $= 0x40020420$. Ее таблица истинности представлена ниже:

00001

01110

10101

11010.

Отметим, что для построения СИ-функций с помощью отображения $AC_{v,i}^{(n)}$, необходимо использовать векторы v веса $wt(v) = \frac{wt(f)}{2}$. Это следует из Предложения 1.

Аналогичным образом можно рассмотреть функцию $DC_i(f)$ для $i = 4$. Получим СИ-функцию h' от 3-х переменных $h'(x_1, x_2, x_3) = 0x96$:

000

011

101

110.

Также рассмотрим случай, когда значение отображения DC_i не равно Λ . Пусть $f(x_1, x_2, x_3, x_4) = 0x8181, i = 1$. Тогда таблица истинности функции f следующая:

0000
0111
1000
1111.

После применения отображения она будет иметь следующий вид:

000
111
000
111

Появление одинаковых наборов означает, что $DC_1(f) = \Lambda$.

Так для предыдущего примера для функции $f(x_1, x_2, x_3, x_4) = 0x8124$ справедливо следующее представление в ДНФ: $f(x_1, x_2, x_3, x_4) = \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4 \vee \bar{x}_1x_2x_3x_4 \vee x_1\bar{x}_2x_3\bar{x}_4 \vee x_1x_2\bar{x}_3x_4$. После применения отображения $AC_{v,5}^{(4)}$ к функции f к каждому конъюнкту в совершенной ДНФ функции g приписывается или переменная x_5 , или ее отрицание $\bar{x}_5$:

$$g(x_1, x_2, x_3, x_4, x_5) = \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4x_5 \vee \bar{x}_1x_2x_3x_4\bar{x}_5 \vee x_1\bar{x}_2x_3\bar{x}_4x_5 \vee x_1x_2\bar{x}_3x_4\bar{x}_5.$$

Для функции h' , полученную выше с помощью отображения DC_i , справедливо следующее представление: $h'(x_1, x_2, x_3) = \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1\bar{x}_2x_3 \vee x_1x_2\bar{x}_3$.

2.4 Критерий равенства получаемых CI-функций при использовании отображения AC^w

Применяя отображение $AC_{v,i}^w$ с разными значениями добавляемых вектор-столбцов v и номеров столбцов i к одной и той же функции от n переменных, можно получить одинаковые функции от $n+1$ переменной. Введем следующие обозначения.

Рассмотрим функцию $f \in CI(n)$, $wt(f) = w$. Обозначим её таблицу истинности T_f :

$$T_f = \begin{pmatrix} u_1^{(1)} & u_1^{(2)} & \dots & u_1^{(n)} \\ u_2^{(1)} & u_2^{(2)} & \dots & u_2^{(n)} \\ \dots & & & \\ u_w^{(1)} & u_w^{(2)} & \dots & u_w^{(n)} \end{pmatrix}$$

где $u_j^{(i)}$ — элемент таблицы истинности T_f , находящийся на пересечении i -го столбца и j -ой строки.

Пусть $a = (a^{(1)}, \dots, a^{(w)})^T$, $b = (b^{(1)}, \dots, b^{(w)})^T$ — вектор-столбцы длины w .

Рассмотрим функции

$$f' = AC_{a,i}^w(f), i \in \{1, n+1\}$$

и

$$f'' = AC_{b,j}^w(f), j \in \{1, n+1\}, \text{ где } i < j.$$

Их таблицы истинности следующие:

$$T_{f'} = \begin{pmatrix} x_1^{(1)} & \dots & x_1^{(i-1)} & a^{(1)} & x_1^{(i)} & \dots & x_1^{(j-1)} & x_1^{(j)} & \dots & x_1^{(n)} \\ x_2^{(1)} & \dots & x_2^{(i-1)} & a^{(2)} & x_2^{(i)} & \dots & x_2^{(j-1)} & x_2^{(j)} & \dots & x_2^{(n)} \\ \dots & & & & & & & & & \\ x_w^{(1)} & \dots & x_w^{(i-1)} & a^{(w)} & x_w^{(i)} & \dots & x_w^{(j-1)} & x_w^{(j)} & \dots & x_w^{(n)} \end{pmatrix}$$

$$T_{f''} = \begin{pmatrix} x_1^{(1)} & \dots & x_1^{(i-1)} & x_1^{(i)} & \dots & x_1^{(j-1)} & b^{(1)} & x_1^{(j)} & \dots & x_1^{(n)} \\ x_2^{(1)} & \dots & x_2^{(i-1)} & x_2^{(i)} & \dots & x_2^{(j-1)} & b^{(2)} & x_2^{(j)} & \dots & x_2^{(n)} \\ \dots & & & & & & & & & \\ x_w^{(1)} & \dots & x_w^{(i-1)} & x_w^{(i)} & \dots & x_w^{(j-1)} & b^{(w)} & x_w^{(j)} & \dots & x_w^{(n)} \end{pmatrix}$$

Далее формулируется критерий равенства функций, являющихся результатом применения отображения $AC_{v,i}^w$.

Теорема 9. *Равенство $f' = f''$ справе тогда и только тогда, когда наборы в исходной таблице истинности T_f функции f можно разбить на пары с номерами $k, t, 1 \leq k \leq w, 1 \leq t \leq w$, для которых выполняются равенства 2.1-2.3:*

$$\begin{cases} x_k^{(1)} x_k^{(2)} \dots x_k^{(i-1)} = x_m^{(1)} x_m^{(2)} \dots x_m^{(i-1)} \\ x_k^{(j)} x_k^{(j+1)} \dots x_k^{(n)} = x_m^{(j)} x_m^{(j+1)} \dots x_m^{(n)} \end{cases} \quad (2.1)$$

$$\begin{cases} x_k^{(i)} = x_m^{(i+1)} \\ x_k^{(i+1)} = x_m^{(i+2)} \\ \dots \\ x_k^{(j-2)} = x_m^{(j-1)} \end{cases} \quad (2.2)$$

$$\begin{cases} a^{(k)} = x_m^{(i)} \\ x_k^{(j-1)} = b^{(m)} \end{cases} \quad (2.3)$$

а для наборов с номерами l , где $l \neq k, m$, которые не вошли в разбиение по парам, должно выполняться условие 2.4:

$$a^{(l)} = x_l^{(i)} = x_l^{(i+1)} = \dots = x_l^{(j-2)} = x_l^{(j-1)} = b^{(l)}. \quad (2.4)$$

Доказательство. Функции равны тогда и только тогда, когда соответствующие им таблицы истинности состоят из одинаковых наборов. Возможны следующие случаи.

1. Одинаковые наборы в таблицах $T_{f'}$ и $T_{f''}$ имеют один и тот же порядковый номер l :

$$\begin{aligned} & x_l^{(1)} x_l^{(2)} \dots x_l^{(i-1)} a^{(l)} x_l^{(i)} \dots x_l^{(j-1)} x_l^{(j)} \dots x_l^{(n)} = \\ & = x_l^{(1)} x_l^{(2)} \dots x_l^{(i-1)} x_l^{(i)} \dots x_l^{(j-1)} b^{(l)} x_l^{(j)} \dots x_l^{(n)}. \end{aligned}$$

Данное равенство справедливо тогда и только тогда, когда для набора с номером l в исходной таблице истинности T_f верно равенство:

$$a^{(l)} = x_l^{(i)} = x_l^{(i+1)} = \dots = x_l^{(j-2)} = x_l^{(j-1)} = b^{(l)}.$$

2. Набор с номером k в таблице истинности T_f' равен набору с номером m в таблице истинности T_f''

$$x_k^{(1)} x_k^{(2)} \dots x_k^{(i-1)} a^{(k)} x_k^{(i)} \dots x_k^{(j-1)} x_k^{(j)} \dots x_k^{(n)} =$$

$$= x_m^{(1)} x_m^{(2)} \dots x_m^{(i-1)} x_m^{(i)} \dots x_m^{(j-1)} b^{(m)} x_m^{(j)} \dots x_m^{(n)}.$$

Данное равенство справедливо тогда и только тогда, когда для наборов с номерами k, m в исходной таблице истинности верны следующие системы равенств:

$$\begin{cases} x_k^{(1)} x_k^{(2)} \dots x_k^{(i-1)} = x_m^{(1)} x_m^{(2)} \dots x_m^{(i-1)} \\ x_k^{(j)} x_k^{(j+1)} \dots x_k^{(n)} = x_m^{(j)} x_m^{(j+1)} \dots x_m^{(n)} \end{cases}$$

$$\begin{cases} x_k^{(i)} = x_m^{(i+1)} \\ x_k^{(i+1)} = x_m^{(i+2)} \\ \dots \\ x_k^{(j-2)} = x_m^{(j-1)} \end{cases}$$

$$\begin{cases} a^{(k)} = x_m^{(i)} \\ x_k^{(j-1)} = b^{(m)} \end{cases}$$

Таким образом, если наборы в исходной таблице истинности T_f можно разбить на пары, для которых указанные системы равенств будут справедливы 2.1-2.3, а для оставшихся наборов будут выполняться равенства 2.4, то при добавлении столбцов a и b на позиции i и j соответственно в таблицу истинности T_f получатся одинаковые таблицы истинности $T_{f'}$ и $T_{f''}$. Соответствующие этим таблицам функции f' и f'' будут равны.

□

2.5 Верхняя оценка мощности множества CI-функций, получаемых с помощью отображения AC^w

Далее приводится верхняя оценка мощности множества CI-функций, которые получаются из исходной функции при применении отображения $AC_{v,i}^w$.

Теорема 10. Пусть $f \in CI(n)$, $wt(f) = w$. Тогда

$$|M| \leq \binom{w}{w/2} (n+1) - n,$$

где

$$M = \{g = AC_{v,i}^w(f), i \in \{1 \dots n+1\}, v \in V_w : wt(v) = \frac{w}{2}\}.$$

Доказательство. Количество уравновешенных векторов v из пространства V_w , которые могут быть использованы в качестве параметров для отображения AC^w , равно $\binom{w}{w/2}$. Число позиций, на которые можно записать уравновешенные вектора, равно $n+1$.

Следовательно, получаем верхнюю оценку на число получаемых функций:

$$|M| \leq \binom{w}{w/2} (n+1)$$

Пусть столбец $a = (a^{(1)}, \dots, a^{(w)})^T$ добавляется на позицию i , столбец $b = (b^{(1)}, \dots, b^{(w)})^T$ на позицию j . Пусть некоторые полученные функции равны. Воспользуемся критерием равенства функций 9, получаемых при применении отображения AC^w . Рассмотрим случай, когда в некоторых полученных таблицах истинности для всех

наборов выполняется только условие 2.4:

$$a^{(l)} = x_l^{(i)} = x_l^{(i+1)} = \dots = x_l^{(j-2)} = x_l^{(j-1)} = b^{(l)}, l \in [1, w].$$

Рассмотрим случай, когда $j = i + 1, i < n + 1$. Тогда

$$a^{(l)} = x_l^{(i)} = b^{(l)}, l \in [1, w].$$

Значения вектор-столбцов a, b существуют всегда и определяются однозначно для каждого номера i . Всего столбцов в таблице истинности n . Тогда справедлива оценка:

$$|M| \leq \binom{w}{w/2} (n + 1) - n.$$

□

Рассмотрим в качестве примера функцию $f \in MCI(3), wt(f) = 2$, таблица истинности которой следующая:

$$T_f = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Построим множество

$$M = \{g = AC_{v,i}^2(f), i \in \{1, \dots, 4\}, v \in V_2 : wt(v) = 1\}.$$

Существует всего два вектора, которые можно использовать в качестве параметра отображения $AC^2 : a = (01)^T, b = (10)^T$. Применяя к данной функции отображение AC^2 с указанными векторами,

получаем новые функции, таблицы истинности которых следующие:

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} \quad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

Среди полученных таблиц истинности три совпадают с построенными таблицами на предыдущих шагах. Следовательно, множество M состоит из 5 различных функций. Посчитаем верхнюю оценку множества M , используя Теорему 2.5:

$$|M| \leq \binom{2}{1}(3+1) - 3 = 5.$$

Таким образом, верхняя оценка для множества M , полученная согласно 2.5, справедлива, и существуют функции, для которых данная оценка достижима.

В Приложении 4.6 можно найти практические и теоретические значения верхней оценки для множества CI-функций, полученных с помощью отображения $AC_{v,i}^w$. Как видно из приведенных таблиц в приложении 4.6, с увеличением веса исходной функции число равных функций, получаемых с помощью отображения AC^w , растет. Для меньших весов функций верхняя оценка может быть достижимой. Среди CI-функций от 4 переменных существуют всего

1. 7 CI-функций веса 2,

2. 13 CI-функций веса 4,

у которых мощность соответствующего множества M достигает верхней оценки.

Среди минимальных CI-функций от 5 переменных существуют

1. 15 минимальных CI-функций веса 2,

2. 150 минимальных CI-функций веса 4,

3. 372 минимальные CI-функции веса 6,

4. 52 минимальные CI-функции веса 8,

у которых мощность соответствующего множества M достигает верхней оценки.

Среди минимальных CI-функций от 6 переменных существуют

1. 31 минимальная CI-функция веса 2,

2. 1649 минимальных CI-функций веса 4,

3. 45255 минимальных CI-функций веса 6,

4. 500375 минимальных CI-функций веса 8,

у которых мощность соответствующего множества M достигает верхней оценки.

2.6 Нижняя оценка мощности множества CI-функций, получаемых с помощью отображения AC^w

Далее приводится нижняя оценка мощности множества CI-функций, получаемых с помощью отображения AC^w .

Теорема 11. Пусть $f \in CI(n)$, $wt(f) = w$. Тогда

$$|M| \geq 2 \binom{w}{w/2} - 2^{w/2},$$

где

$$M = \{g = AC_{v,i}^w(f), i \in \{1 \dots n+1\}, v \in V_w : wt(v) = \frac{w}{2}\}.$$

Доказательство. Число уравновешенных векторов из пространства V_w , которое может быть записано в качестве первого столбца, равно $\binom{w}{w/2}$. Таким образом, при добавлении таких векторов на первую позицию получим $\binom{w}{w/2}$ разных функций.

При добавлении столбцов на вторую позицию получим ещё $\binom{w}{w/2}$ функций. Посчитаем максимальное число функций, полученных при добавлении столбцов на вторую позицию, которые могут совпадать с функциями, полученными при добавлении столбцов на первую позицию.

Пусть a и b — добавляемые вектор-столбцы длины w . Обозначим через f' и f'' следующие функции:

$$f' = AC_{a,1}^w(f),$$

$$f'' = AC_{b,2}^w(f).$$

Обозначим T'_f и T''_f соответствующие им таблицы истинности. Рассмотрим все возможные случаи равенства получаемых функций, используя Теорему 9.

1. Пусть для всех наборов таблиц истинности полученных функций выполнено условие 2.4 из теоремы 9:

$$a^l = x_l^1 = b^l, l \in \{1 \dots w\}.$$

Из этого равенства однозначно определяются значения вектор-столбцов a и b . Рассматриваемый случай существует всегда для любой функции. Таким образом, можно получить две равные функции, добавляя в качестве первого и второго столбца вектор-столбец $x_l^{(1)}, l \in [1, w]$.

2. Пусть для части наборов выполняются условия 2.1-2.3 теоремы 9, а для оставшихся наборов выполняется условие 2.4. При этом пусть наборы с номерами k из таблицы истинности T'_f совпадают с наборами с номерами m из таблицы истинности T''_f , а наборы с номерами m из таблицы истинности T'_f совпадают с наборами с номерами k из таблицы истинности T''_f , для любых пар значений k, m :

$$\begin{cases} a^{(k)} x_k^{(1)} x_k^{(2)} \dots x_k^{(n)} = x_m^{(1)} b^{(m)} x_m^{(2)} \dots x_m^{(n)} \\ a^{(m)} x_m^{(1)} x_m^{(2)} \dots x_m^{(n)} = x_k^{(1)} b^{(k)} x_k^{(2)} \dots x_k^{(n)} \end{cases}$$

Будем говорить, что в этом случае номера k, m не пересекаются. Тогда верны следующие равенства:

$$\begin{cases} a^k = x_m^1 \\ a^m = x_k^1 \\ b^k = x_m^1 \\ b^m = x_k^1 \\ x_k^2 x_k^3 \dots x_k^n = x_m^2 x_m^3 \dots x_m^n \\ a^l = x_l^1 = b^l, l \neq \{m, k\}. \end{cases}$$

Предположим, что исходное множество наборов можно разбить на пары с непересекающимися номерами несколькими способами: пусть существует набор с номером k из таблицы истинности T'_f , совпадающий с набором с номером m из таблицы истинности T''_f для одного разбиения на пары, и совпадающий с набором с номером t из таблицы истинности T''_f для другого разбиения, для любых значений $k, m, t \in [1, w]$. Тогда по Теореме 9 верно:

$$\begin{cases} a^{(k)} x_k^{(1)} x_k^{(2)} \dots x_k^{(n)} = x_m^{(1)} b^{(m)} x_m^{(2)} \dots x_m^{(n)} \\ a^{(k)} x_k^{(1)} x_k^{(2)} \dots x_k^{(n)} = x_t^{(1)} b^{(t)} x_t^{(2)} \dots x_t^{(n)} \end{cases}$$

Из равенств видно, что в этом случае два набора в исходной таблице истинности должны совпадать. Получаем противоречие. Значит, если существует разбиение исходного множества наборов на пары с непересекающимися номерами, то это разбиение единственно.

Так как разбиение на пары с непересекающимися номерами единственно, то число возможных способов выбрать из разбиения пары для рассматриваемого случая равно

$$\sum_{i=1}^{w/2} = \binom{w/2}{i},$$

где $w/2$ — число пар в исходной таблице истинности.

3. Пусть для части наборов выполняются условия 2.1-2.3 Теоремы 9. При этом пусть

- наборы с номерами k_1 из таблицы истинности T'_f совпадают с наборами с номерами k_2 из таблицы истинности T''_f ,
- наборы с номерами k_2 из таблицы истинности T'_f совпадают с наборами с номерами k_3 из таблицы истинности T''_f ,
- наборы с номерами k_3 из таблицы истинности T'_f совпадают с наборами с номерами k_1 из таблицы истинности T''_f :

$$\begin{cases} a^{k_1} x_{k_1}^2 x_{k_1}^3 \dots x_{k_1}^n = x_{k_2}^2 b^{k_2} x_{k_2}^3 \dots x_{k_2}^n \\ a^{k_2} x_{k_2}^2 x_{k_2}^3 \dots x_{k_2}^n = x_{k_3}^2 b^{k_3} x_{k_3}^3 \dots x_{k_3}^n \\ a^{k_3} x_{k_3}^2 x_{k_3}^3 \dots x_{k_3}^n = x_{k_1}^2 b^{k_1} x_{k_1}^3 \dots x_{k_1}^n \end{cases}$$

Тогда верно:

$$\begin{cases} x_{k_1}^2 x_{k_1}^3 \dots x_{k_1}^n = x_{k_2}^2 x_{k_2}^3 \dots x_{k_2}^n \\ x_{k_2}^2 x_{k_2}^3 \dots x_{k_2}^n = x_{k_3}^2 x_{k_3}^3 \dots x_{k_3}^n \\ x_{k_3}^2 x_{k_3}^3 \dots x_{k_3}^n = x_{k_1}^2 x_{k_1}^3 \dots x_{k_1}^n \end{cases}$$

Из приведенных равенств видно, что в этом случае в исходной таблице истинности должно быть два одинаковых набора, что

невозможно. Очевидно, что чем больше таких пар наборов, тем больше число одинаковых наборов в исходной таблице истинности. Поэтому данный случай не является возможным.

Таким образом, максимальное количество функций, получаемых при добавлении столбцов на вторую позицию, которые могут совпасть с функциями, полученными ранее при добавлении столбцов на первую позицию равно

$$1 + \sum_{i \in [1, w/2]} \binom{w/2}{i} = 2^{w/2}.$$

Тогда верно следующее неравенство:

$$|M| \geq 2 \binom{w}{w/2} - 2^{w/2}.$$

Так как рассуждения были рассмотрены лишь для добавлений столбцов на первую и вторую позиции, то данная оценка не зависит от n .

□

Рассмотрим в качестве примера функцию $f \in MCI(4)$, $wt(f) = 2$, таблица истинности которой следующая:

$$T_f = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Построим множество

$$M' = \{f' = AC_{a,1}^2(f), f'' = AC_{b,2}^2(f), wt(a) = wt(b) = 1\}.$$

Множество M' является подмножеством множества M и состоит из функций, таблицы истинности которых представлены ниже:

$$\begin{pmatrix} \mathbf{0} & 0 & 1 & 0 & 0 \\ \mathbf{1} & 1 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & \mathbf{0} & 1 & 0 & 0 \\ 1 & \mathbf{1} & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{1} & 0 & 1 & 0 & 0 \\ \mathbf{0} & 1 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & \mathbf{1} & 1 & 0 & 0 \\ 1 & \mathbf{0} & 0 & 1 & 1 \end{pmatrix}$$

Среди полученных таблиц истинности одна совпадает с построенной таблицей на предыдущем шаге. Следовательно, множество M' состоит из 3 различных функций. Посчитаем нижнюю оценку множества M , используя Теорему 11:

$$|M| \geq |M'| \geq 2 \cdot \binom{2}{1} - 2 = 2.$$

Таким образом, данная оценка из Теоремы 11 справедлива.

Рассмотрим еще один пример. Пусть $f \in MCI(3)$, $wt(f) = 4$, таблица истинности которой следующая:

$$T_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Построим множество

$$M' = \{f' = AC_{a,1}^4(f), f'' = AC_{b,2}^4(f), wt(a) = wt(b) = 2\}.$$

Множество M' является подмножеством множества M и состоит

из функций, таблицы истинности которых представлены ниже:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Среди полученных таблиц истинности четыре совпадают с построенными таблицами на предыдущих шагах. Следовательно, множество M' состоит из 8 различных функций. Посчитаем нижнюю оценку множества M , используя Теорему 11:

$$|M| \geq |M'| = 2 \cdot \binom{4}{2} - 4 = 8.$$

В Приложении 4.6 можно найти практические и теоретические значения нижней оценки для множества СИ-функций от 4, 5, 6 переменных, полученных с помощью отображения $AC_{v,i}^w$.

2.7 Результаты применения предложенного метода построения СИ-функций

В данной главе приводятся примеры использования предложенного метода построения СИ-функций.

Приведенные ниже СИ-функции были построены по следующему алгоритму. К минимальным СИ-функциям от малого числа переменных был применен предложенный метод построения функций, в результате чего были получены минимальные СИ-функции от большого числа переменных. После этого были рассмотрены возможные суммы полученных минимальных СИ-функций от большого числа переменных с попарно непересекающимися носителями и получены некоторые СИ-функции от большого числа переменных.

Сами минимальные СИ-функции от малого числа переменных находились с помощью перебора, были использованы результаты главы 2.8.

Таким образом, удалось построить 4-устойчивую функцию f_0 от 7 переменных. Данная функция раскладывается в сумму 4 минимальных СИ-функций от 7 переменных веса 4 и 8 минимальных СИ-функций от 7 переменных веса 6. Любая пара среди функций из разложения f_0 удовлетворяет условию: $g \cdot h = 0$. Рассматриваемые минимальные СИ-функции от 7 переменных были построены из известных минимальных СИ-функций весов 4 и 6 от малого числа переменных. Вектор значений функции f_0 и ее параметры представлены ниже (все векторы значений представлены в шестнадцатичном виде).

$$f_0 = 0x5aa5a55a6699996699666699a55a5aa5$$

$wt(f_0) = 64$	$cor(f_0) = 4$	$deg(f_0) = 2$	$nl(f_0) = 32$	$\rho(f_0) = 0$
----------------	----------------	----------------	----------------	-----------------

Эта функция достигает верхней границы нелинейности для 4-устойчивых функций от 7 переменных ([38]).

Также от 7 переменных была построена 2-устойчивая функция f_1 , не являющаяся алгебраически вырожденной. Данная функция раскладывается в сумму 1 минимальной СИ-функций от 7 переменных веса 2, 2 минимальных СИ-функций от 7 переменных веса 4 и 9 минимальных СИ-функций от 7 переменных веса 6. Любая пара среди функций из разложения f_1 удовлетворяет условию: $g \cdot h = 0$. Рассматриваемые минимальные СИ-функции от 7 переменных были построены из известных минимальных СИ-функций весов 2, 4 и 6 от малого числа переменных.

$$f_1 = 0x1bd83cc31bd869969669e427c33ce427$$

$wt(f_1) = 64$	$cor(f_1) = 2$	$deg(f_1) = 3$	$nl(f_1) = 48$	$\rho(f_1) = 16$
----------------	----------------	----------------	----------------	------------------

Аналогичным образом построена 4-устойчивая функция f_2 от 8 переменных. Данная функция раскладывается в сумму 11 минимальных СИ-функций от 8 переменных веса 10, 1 минимальной СИ-функции от 8 переменных веса 8, 1 минимальной СИ-функции от 8 переменных веса 6 и 2 минимальных СИ-функций от 8 переменных веса 2. Любая пара среди функций из разложения f_2 удовлетворяет условию: $g \cdot h = 0$. Рассматриваемые минимальные СИ-функции

от 8 переменных были построены из известных минимальных СИ-функций весов 2, 6, 8 и 10 от малого числа переменных. Вектор значений функции f_2 и ее параметры представлены ниже.

$$f_2 = 0xc93696c33c69639c639c3c6996c3c936 \\ 639c3c6996c3c936c93696c33c69639c$$

$wt(f_2) = 128$	$cor(f_2) = 4$	$deg(f_2) = 3$	$nl(f_2) = 64$
-----------------	----------------	----------------	----------------

Также функцию f_2 можно получить, рассматривая сумму 15 минимальных СИ-функций от 8 переменных веса 8, 1 минимальной СИ-функции от 8 переменных веса 6 и 1 минимальной СИ-функции от 8 переменных веса 2.

Построена 5-устойчивая функция f_3 от 9 переменных. Функция раскладывается в сумму 41 минимальных СИ-функций от 9 переменных веса 6, 1 минимальной СИ-функции от 9 переменных веса 4 и 3 минимальных СИ-функций от 9 переменных веса 2. Любая пара среди функций из разложения f_3 удовлетворяет условию: $g \cdot h = 0$. Рассматриваемые минимальные СИ-функции от 9 переменных были построены из известных минимальных СИ-функций весов 2, 4, и 6 от малого числа переменных. Вектор значений функции f_3 и ее параметры представлены ниже.

$$f_3 = 0x36c9693cc3969c639c63c396693c36c9$$

$$c93696c33c69639c639c3c6996c3c936$$

$$c93696c33c69639c639c3c6996c3c936$$

$$36c9693cc3969c639c63c396693c36c9$$

$wt(f_3) = 256$	$cor(f_3) = 5$	$deg(f_3) = 3$	$nl(f_3) = 128$
-----------------	----------------	----------------	-----------------

Ниже представлена 7-устойчивая функция f_4 от 10 переменных. Функция раскладывается в сумму 83 минимальных CI-функций от 10 переменных веса 6, 2 минимальных CI-функций от 10 переменных веса 4 и 3 минимальных CI-функций от 10 переменных веса 2. Любая пара среди функций из разложения f_4 удовлетворяет условию: $g \cdot h = 0$. Рассматриваемые минимальные CI-функции от 10 переменных были построены из известных минимальных CI-функций весов 2, 4 и 6 от малого числа переменных.

$$f_4 = 0x96696996699696699669699669969669$$

$$69969669966969966996699669966996$$

$$96696996699696696996699669966996$$

$$96696996699696696996699669966996$$

$$69969669966969969669699669969669$$

$$69969669966969969669699669969669$$

$$69969669966969969669699669966996$$

$$96696996699696699669699669969669$$

$wt(f_4) = 512$	$cor(f_4) = 7$	$deg(f_4) = 2$	$nl(f_4) = 256$
-----------------	----------------	----------------	-----------------

Эта функция достигает верхней границы нелинейности для 7-устойчивых функций (см., например, [19]). При этом функции с такими параметрами могут быть построены также с помощью метода из работы [19].

Аналогичным способом были построены 4 и 6-устойчивые функции, раскладывающиеся в сумму минимальных СИ-функций от 11 переменных веса 4, среди которых любая пара функций удовлетворяет условию: $g \cdot h = 0$. Из построенных устойчивых функций от 11 переменных векторы значений и параметры двух функций f_5 и f_6 представлены ниже.

$$f_5 = 0xc93696c33c69639c639c3c6996c3c936$$

$$36c9693cc3969c639c63c396693c36c9$$

$$639c3c6996c3c9369c63c396693c36c9$$

$$c93696c33c69639c36c9693cc3969c63$$

$$c93696c33c69639c639c3c6996c3c936$$

$$36c9693cc3969c639c63c396693c36c9$$

$$639c3c6996c3c9369c63c396693c36c9$$

$$c53a5ac33ca5a35c3ac5a53cc35a5ca3$$

$$3ac5a53cc35a5ca3c53a5ac33ca5a35c$$

$$9c63c396693c36c9639c3c6996c3c936$$

$$9c63c396693c36c936c9693cc3969c63$$

$$639c3c6996c3c936c93696c33c69639c$$

$$36c9693cc3969c63c93696c33c69639c$$

$$9c63c396693c36c9639c3c6996c3c936$$

$$9c63c396693c36c936c9693cc3969c63$$

$$639c3c6996c3c936c93696c33c69639c$$

$wt(f_5) = 1024$	$cor(f_5) = 4$	$deg(f_5) = 6$	$nl(f_5) = 768$
------------------	----------------	----------------	-----------------

$$f_6 = 0xc93696c33c69639c639c3c6996c3c936$$

$$36c9693cc3969c639c63c396693c36c9$$

$$639c3c6996c3c9369c63c396693c36c9$$

$$c93696c33c69639c36c9693cc3969c63$$

$$c53a5ac33ca5a35ca35c3ca55ac3c53a$$

$$3ac5a53cc35a5ca35ca3c35aa53c3ac5$$

$$a35c3ca55ac3c53a5ca3c35aa53c3ac5$$

$$c53a5ac33ca5a35c3ac5a53cc35a5ca3$$

$$3ac5a53cc35a5ca3c53a5ac33ca5a35c$$

$$5ca3c35aa53c3ac5a35c3ca55ac3c53a$$

$$5ca3c35aa53c3ac53ac5a53cc35a5ca3$$

$$a35c3ca55ac3c53ac53a5ac33ca5a35c$$

$$36c9693cc3969c63c93696c33c69639c$$

$$9c63c396693c36c9639c3c6996c3c936$$

$$9c63c396693c36c936c9693cc3969c63$$

$$639c3c6996c3c936c93696c33c69639c$$

$wt(f_6) = 1024$	$cor(f_6) = 6$	$deg(f_6) = 4$	$nl(f_6) = 768$
------------------	----------------	----------------	-----------------

2.8 Построение классификации минимальных СИ-функций и СИ-функций от 4, 5 и 6 переменных относительно группы Джевонса

Для использования предложенного метода построения СИ-функций необходимо наличие известных СИ-функций, которые будут использоваться как «стартовые» точки. В качестве таких исходных функций можно использовать СИ-функции от 4, 5 и 6 переменных. Использование минимальных СИ-функций и их свойств может существенно упростить задачу построения СИ-функций, так как с помощью них можно построить любую СИ-функцию от рассматриваемого числа переменных. Используя известные оценки на порядок корреляционной иммунности и вес минимальных СИ-функций (см. Теоремы 4, 5), можно сократить этот перебор. Кроме того, составление классификации относительно группы Джевонса позволяет изучить свойства множества СИ-функций в целом.

2.8.1 Построение классификации минимальных СИ-функций и СИ-функций от 4 переменных относительно группы Джевонса

Ниже представлены мощности множества СИ-функций и множества минимальных СИ-функций от 4 переменных, а также число классов эквивалентности относительно группы Джевонса.

- $|CI(4)| = 648$
- $|\widehat{CI}(4)| = 23$
- $|MCI(4)| = 32$

- $|\widehat{MCI}(4)| = 2$

Ниже представлены некоторые характеристики классификации СИ-функций и минимальных СИ-функций от 4 переменных относительно группы Джевонса.

w	$ \widehat{CI^w}(4) $	$ CI^w(4) $	c	$ \widehat{CI_c}(4) $	$ CI_c(4) $	$ \widehat{CI_c^8}(4) $	$ CI_c^8(4) $
0	1	1	1	19	636	5	212
2	1	8	2	1	8	1	8
4	3	52	3	1	2	1	2
6	3	152	4	2	2	0	0
8	7	222					

w	$ \widehat{MCI^w}(4) $	$ MCI^w(4) $
2	1	8
4	1	24

Полную классификацию СИ-функций от 4 переменных можно найти в Приложении 4.4. Перечисление всех минимальных СИ-функций от 4 переменных можно найти в Приложении 4.5. Классификация минимальных СИ-функций от 4 переменных представлена ниже.

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$	$\rho(f)$	$\delta(f)$	$ f^{\mathcal{D}_n} $
0x0180	2	3	2	1	0	0	8
0x0690	4	2	4	1	0	0	24

2.8.2 Построение классификации минимальных СИ-функций и СИ-функций от 5 переменных относительно группы Джевонса

Ниже представлены мощности множества СИ-функций и множества минимальных СИ-функций от 5 переменных, а также число классов эквивалентности относительно группы Джевонса.

- $|CI(5)| = 3140062$
- $|\widehat{CI}(5)| = 1524$
- $|MCI(5)| = 1240$
- $|\widehat{MCI}(5)| = 6$

Ниже представлены некоторые характеристики классификации СИ-функций и минимальных СИ-функций от 5 переменных относительно группы Джевонса.

w	$ \widehat{CI}^w(5) $	$ CI^w(5) $	c	$ \widehat{CI}_c(5) $	$ CI_c(5) $	$ \widehat{CI}_c^{16}(5) $	$ CI_c^{16}(5) $
0	1	1	1	1511	3139004	359	807428
2	1	16	2	9	1044	5	540
4	4	320	3	1	10	1	10
6	8	3824	4	1	2	1	2
8	36	27640	5	2	2	0	0
10	73	123600					
12	190	353120					
14	266	657520					
16	366	807980					

w	$ \widehat{MCI^w(5)} $	$ MCI^w(5) $
2	1	16
4	2	200
6	2	864
8	1	160

Из таблиц видно, что количество классов эквивалентности достаточно велико, поэтому приведем примеры лишь некоторых представителей классов. Рассмотрим тех представителей классов эквивалентности, у которых порядок корреляционной иммунности равен 2, 3 и 4.

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$	$\rho(f)$	$\delta(f)$	$ f^{\mathcal{D}_n} $
0x06609009	8	2	8	2	0	0	60
0x1698a443	12	3	12	2	6	6	192
0x0ff0f00f	16	1	0	2	0	0	20
0x17e8e817	16	2	8	2	0	0	80
0x1bd8e427	16	2	8	2	0	0	120
0x1be4e41b	16	2	8	2	0	0	240
0x1ee1e11e	16	2	8	2	0	0	80
0x3cc3c33c	16	1	0	3	0	0	10
0x69969669	16	1	0	4	0	0	2
0x3ddae697	20	3	12	2	6	6	192
0x6ff6f99f	24	2	8	2	0	0	60

Классификация минимальных СИ-функций от 5 переменных представлена ниже.

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$	$\rho(f)$	$\delta(f)$	$ f^{\mathcal{D}_n} $
0x00018000	2	4	2	1	0	0	16
0x00069000	4	3	4	1	0	0	80
0x00182400	4	3	4	1	0	0	120
0x01186008	6	4	6	1	4	4	480
0x01188240	6	4	6	1	4	4	384
0x01686801	8	3	8	1	0	0	160

2.8.3 Построение классификации минимальных СИ-функций от 6 переменных относительно группы Джевонса

Перечисление СИ-функций от 6 переменных и больше с использованием персонального компьютера является на сегодняшний день не осуществимой задачей в силу невозможности совершения полного перебора всех функций от указанного числа переменных. Поэтому в работе рассматриваются минимальные СИ-функций от 6 переменных.

Данные функции могут быть использованы в качестве исходных функций для построения минимальных СИ-функций от большего числа переменных. Использование минимальных СИ-функций от 6 переменных более выгодно по сравнению с использованием минимальных СИ-функций от 4 и 5 переменных, так как они позволяют строить функции больших весов от большего числа переменных.

Сформулируем гипотезу, в предположении справедливости которой построена классификация.

Гипотеза 1. *Если не существует минимальных СИ-функций четного веса w от n переменных, то не существует минимальных СИ-функций веса большего w от этого же числа переменных.*

Ниже приведено количество СИ-функций веса 2, 4, 6, 8, 10, 12, 14, 16 от 6 переменных:

- $|CI^2(6)| = 32$
- $|CI^4(6)| = 1936$
- $|CI^6(6)| = 83680$
- $|CI^8(6)| = 2452080$
- $|CI^{10}(6)| = 49585440$
- $|CI^{12}(6)| = 712645616$
- $|CI^{14}(6)| = 7472934880$
- $|CI^{16}(6)| = 58431976800$

Ограничения по времени вычисления СИ-функций начинают действовать для функций большего веса. Однако, при подсчете числа минимальных СИ-функций от 6-ти переменных было выявлено, что минимальных СИ-функций веса больше 10 не существует. С учетом Гипотезы 1 множество СИ-функций с указанными выше весами от 6 переменных полностью содержит множество минимальных СИ-функций от 6 переменных. В предположении Гипотезы 1 о минимальных СИ-функциях можно сделать следующие выводы:

- $|MCI(6)| = 38400$
- $|\widehat{MCI}(6)| = 109$

В силу большого количества классов эквивалентности ниже приведем лишь представителей некоторых классов.

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$
0x8000000000000001	2	5	2	1
0x4000000000000002	2	5	2	1
0x6000000000000009	4	4	4	1
0x4200000000000081	4	4	4	1
0x2840000000004003	6	5	6	1
0x2440000000002009	6	5	6	1
0x1880800010000007	8	4	8	1
0x1480800002000043	8	4	8	1
0x1680800080000017	10	5	10	1
0x4081810002100428	10	5	10	1

Обозначим $\widehat{MCI}(n, wt, deg, nl)$ — множество всех классов эквивалентности минимальных CI-функций n переменных относительно группы Джевонса, у которых вес равен wt , степень и нелинейность равны deg и nl соответственно.

wt	deg	nl	$cor(f)$	$ \widehat{MCI}(6, wt, deg, nl) $
2	5	2	1	2
4	4	4	1	3
6	5	6	1	10
8	4	8	1	54
10	5	10	1	40

Данные функции от 6 переменных были построены следующим образом. С помощью полного перебора были сгенерированы все возможные функции от 5 переменных. Далее были рассмотрены все возможные конкатенации пар функций от 5 переменных одинакового веса. Конкатенация векторов значений таких пар является функцией

четного веса от 6 переменных. Так как задача заключалась в построении классификации минимальных СИ-функций, для которых верна Теорема 5, то далее проверялось: являются ли построенные функции от 6 переменных корреляционно-иммунными. Проверка осуществлялась с помощью критерия корреляционной иммунности (см. Теорему 1). Далее, если функция являлась корреляционно-иммунной, то проверялось: минимальна она или нет. Проверка осуществлялась с помощью критерия минимальности корреляционно-иммунных функций (см. Теорему 3).

Построение СИ-функций от большего числа переменных с помощью данного метода с использованием персонального компьютера не представляется возможным.

Глава 3

Комбинаторные и спектральные свойства минимальных CI-функций

В данной главе доказываются свойства минимальных CI-функций.

3.1 Достаточное условие существования минимальных CI-функций

Докажем следующее условие существования минимальных CI-функций.

Предложение 6. *Если существует минимальная CI-функция веса w от n переменных, то существует минимальная CI-функция веса w от k переменных, для любого $k > n$.*

Доказательство. Для доказательства утверждения достаточно применить несколько раз отображение $AC_{v,i}^{(w)}$ для некоторых v и i , где $wt(v) = \frac{w}{2}$ к исходной минимальной CI-функции и заметить, что после применения отображения $AC_{v,i}^{(w)}$ вес функций сохраняется. $\square$

Следствие 2. *Для любого $n \geq 5$ существуют минимальные CI-функции веса 6 и веса 8.*

Доказательство. Для доказательства существования минимальных CI-функций веса 6 и 8 от 5-ти переменных воспользуемся результатами работы [4]. Рассмотрим минимальную CI-функцию от 5-ти

переменных веса 6:

$$f(x_1, x_2, x_3, x_4, x_5) = 0x01186008.$$

Далее, используя отображение $AC_{v,i}^w(f)$ и учитывая то, что вес функций сохраняется после применения отображения, для любого вектора v , для которого верно $wt(v) = \frac{wt(f)}{2}$, можно построить минимальные CI-функции от большего числа переменных веса 6.

Также рассмотрим функцию от 5-ти переменных веса 8:

$$f(x_1, x_2, x_3, x_4, x_5) = 0x01686801.$$

Эта функция является минимальной CI-функцией веса 8. Далее, аналогично используем отображение $AC_{v,i}^w(f)$ и его свойства для любых векторов v , вес которых равен $\frac{wt(f)}{2}$, получаем искомую функцию. $\square$

Следствие 3. *Для любого $n \geq 6$ существуют минимальные CI-функции веса 10.*

Доказательство. Доказательство аналогично предыдущему. В качестве исходной функции, к которой будет применяться отображение, рассмотрим минимальную CI-функцию от 6-ти переменных веса 10:

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = 0x0006128082100440.$$

$\square$

3.2 Спектральный критерий минимальности СИ-функций

Для определения, является ли СИ-функция минимальной или нет, предлагается следующий критерий.

Предложение 7. *(спектральный критерий минимальности СИ-функций) Для функции $f \in \mathcal{F}_n$ введем множество*

$$M_f = \{g \in \mathcal{F}_n : \text{supp}(g) \subset \text{supp}(f), g \neq 0, g \neq f, \\ \text{wt}(g) - \text{четное число} \}$$

— множество подфункций функции f от n переменных четного веса. Тогда СИ-функция f является минимальной СИ-функцией от n переменных тогда и только тогда, когда

$$\prod_{\forall g \in M_f} \sum_{u, \text{wt}(u)=1} W_g^2(u) \neq 0.$$

Доказательство. Функция является СИ-функцией тогда и только тогда, когда ее коэффициент Уолша для всех векторов u , вес которых равен единице, равен нулю (см. Теорему 1). Из этого критерия следует, что функция является СИ-функцией тогда и только тогда, когда сумма всех квадратов коэффициентов по всем векторам u равна нулю: $\sum_{u, \text{wt}(u)=1} W_f^2(u) = 0$.

Далее, функция является минимальной тогда и только тогда, когда из носителя этой функции нельзя выделить подмножество четной мощности, которое является носителем СИ-функции, то есть тогда и только тогда, когда для любого собственного подмножества но-

сителя четной мощности рассматриваемой CI-функции сумма квадратов коэффициентов Уолша соответствующей функции не равна нулю.

Следовательно, функция является минимальной CI-функцией, если выполнено условие:

$$\prod_{\forall g \in M_f} \sum_{u, wt(u)=1} W_g^2(u) \neq 0.$$

С другой стороны, перебрав все собственные подмножества носителя CI-функции, посчитав для каждого указанную сумму квадратов коэффициента Уолша и сравнив её с нулем, то есть проверив следующее неравенство:

$$\prod_{\forall g \in M_f} \sum_{u, wt(u)=1} W_g^2(u) \neq 0,$$

можно определить: является ли CI-функция минимальной или нет.

□

3.3 Существенные переменные минимальных CI-функций

Для построения любой булевой функции необходимо задать её вектор значений с точностью до всех существенных переменных. Доказанная ниже теорема показывает, что минимальную CI-функцию от n переменных нельзя описать с помощью функции от $n - 1$ переменной.

Предложение 8. *Любая минимальная CI-функция существенно*

зависит от всех своих переменных.

Доказательство. Пусть $f \in MCI(n)$ — минимальная CI-функция. Доказательство проведем от противного. Предположим, что у функции есть фиктивная переменная. Не ограничивая общности рассуждений, будем считать, что x_1 — это фиктивная переменная. Тогда обозначим $f(0, x_2, \dots, x_n) = f(1, x_2, \dots, x_n) = f_1$.

Покажем, что функция $f_1 \in CI(n-1)$. Число нулей в любом i -ом столбце, где $2 \leq i \leq n$, в таблице истинности функции f равно удвоенному числу нулей в i -ом столбце функции f_1 . Аналогично для числа единиц. В таблице истинности исходной функции все столбцы уравновешенны, а значит все столбцы в таблице истинности функции f_1 также уравновешенны. Кроме того, наборы составляющие таблицу истинности функции f_1 различны. Значит, $f_1 \in CI(n-1)$ (см. Следствие 1).

Покажем, как можно выделить из функции f подфункцию, являющуюся корреляционно-иммунной. Разобьем произвольным образом на два равномоощных непересекающихся множества носитель функции f_1 :

$$A_1 \cup A_2 = \text{supp}(f_1),$$

$$|A_1| = |A_2|,$$

$$A_1 \cap A_2 = \emptyset.$$

Тогда положим

$$\begin{aligned} \text{supp}(g) = \{ & (0, x_2, \dots, x_n) : (x_2, \dots, x_n) \in A_1 \} \cup \\ & \cup \{ (1, x_2, \dots, x_n) : (x_2, \dots, x_n) \in A_2 \}. \end{aligned}$$

Функция g является CI-функцией, так как все столбцы в таблице истинности уравновешенны: первый столбец уравновешен, так как $|A_1| = |A_2|$, а остальные являются столбцами таблицы истинности функции f_1 , а значит тоже уравновешенны. Кроме того, $\text{supp}(g) \subset \text{supp}(f)$. Получаем противоречие с условием $f \in MCI(n)$.

□

3.4 Весовые свойства минимальных CI-функций

Приведенная ниже теорема улучшает оценку для веса минимальных CI-функций, доказанную в работе [1].

Предложение 9. Пусть $f \in MCI(n)$, $n \geq 4$. Тогда $wt(f) < 2^{n-1} - 2$.

Доказательство. Теорему докажем от противного. Предположим, что теорема неверна, то есть существует по крайней мере одна минимальная CI-функция от $n \geq 4$ переменных, вес которой $wt(f) \geq 2^{n-1} - 2$. Учитывая оценку на вес минимальных CI-функций из работы [1] ($wt(f) < 2^{n-1}$, где $n \geq 4$) и то, что значение веса функции есть целое число, получаем, что существует минимальная CI-функция веса $wt(f) = 2^{n-1} - 2$ от $n \geq 4$ переменных. Построим такую функцию f как конкатенацию двух функций f_1 и f_2 и покажем, что построение такой функции приводит к противоречию с условием теоремы.

Рассмотрим всевозможные лексикографически упорядоченные наборы от n переменных. Всего таких наборов 2^n . Среди первых 2^{n-1} наборов выберем произвольным образом $2^{n-2} - 1$ наборов. Пусть эти наборы являются носителем функции f_1 . Вес функции f_1 определяется количеством этих наборов, то есть $wt(f_1) = \frac{wt(f)}{2} = 2^{n-2} - 1$.

Построим теперь носитель функции f_2 . Заметим, что если $f \in CI(n)$, $f = f_1 || f_2$, то $wt(f_1) = wt(f_2) = \frac{wt(f)}{2}$. Лексикографически упорядочим множество всех оставшихся 2^{n-1} наборов и представим их в виде таблицы T .

Из оставшихся 2^{n-1} наборов нельзя использовать те наборы, которые при сложении по модулю два с наборами из носителя функции f_1 дают значение 1, так как иначе заведомо будет построена не минимальная CI-функция. Также при выборе наборов носителя функции f_2 необходимо учитывать то, что у результирующей таблицы истинности построенной функции f все столбцы должны быть уравновешенны (см. Следствие 1). Это значит, что выбрав столбец в таблице истинности функции f_1 и приписав к нему соответствующий столбец из таблицы истинности функции f_2 , итоговый столбец таблицы истинности функции f должен содержать одинаковое количество нулей и единиц.

Не ограничивая общности рассуждений, рассмотрим i -ый столбец таблицы истинности функции f_1 , где $i \neq 1$ (нумерация ведется слева направо). Первый столбец не рассматривается, так как в силу исходной упорядоченности 2^n наборов первый столбец таблицы истинности функции f_1 состоит из нулей, а первый столбец таблицы истинности функции f_2 соответственно из единиц.

Пусть x — количество нулей в рассматриваемом i -ом столбце. Тогда $2^{n-2} - 1 - x$ — количество единиц в i -ом столбце. Удалим из оставшихся наборов те наборы, которые при сложении с наборами из носителя функции f_1 дают 1, так как иначе будет построена заведомо не минимальная CI-функция (см. Теорему 3). С точки зрения i -го столбца это значит, что необходимо удалить $2^{n-2} - 1 - x$ нулей и x единиц. Обозначим T' полученную таблицу после уда-

ления наборов. Тогда i -ый столбец таблицы T' будет содержать $2^{n-2} - (2^{n-2} - 1 - x) = 1 + x$ нулей и $2^{n-2} - x$ единиц (до удаления наборов все столбцы таблицы T , кроме первого, имеют 2^{n-2} единиц и нулей). С другой стороны, учитывая, что итоговый i -ый столбец таблицы истинности функции f должен быть уравновешенным, в результирующем i -ом столбце таблицы истинности функции f_2 должны быть x единиц и $2^{n-2} - 1 - x$ нулей. В следующей таблице показано оставшееся число нулей и единиц в i -ом столбце таблицы T' и необходимое их количество в i -ом столбце таблиц истинности функций f_1 и f_2 :

	$supp(f_1)$	T'	$supp(f_2)$
0	x	$1 + x$	$2^{n-2} - 1 - x$
1	$2^{n-2} - 1 - x$	$2^{n-2} - x$	x

Очевидно, что количество оставшихся нулей (единиц) в i -ом столбце таблицы T' должно быть больше (либо равно) необходимого количества нулей (единиц) в i -ом столбце таблицы истинности функции f_2 . Откуда получаем следующую систему неравенств:

$$\begin{cases} 1 + x \geq 2^{n-2} - 1 - x \\ 2^{n-2} - x \geq x \end{cases}$$

$$\begin{cases} x \leq 2^{n-3} \\ x \geq 2^{n-3} - 1 \end{cases}$$

Так как x — целое число, то $x \in \{2^{n-3} - 1, 2^{n-3}\}$. Если количество нулей в i -ом столбце таблицы истинности функции f_1 равно $2^{n-3} - 1$, тогда количество единиц в этом столбце равно 2^{n-3} . Аналогично, ес-

ли количество нулей в i -ом столбце таблицы истинности функции f_1 равно 2^{n-3} , то число единиц в этом столбце равно $2^{n-3} - 1$. Поэтому, не ограничивая общности рассуждений, пусть $x = 2^{n-3} - 1$. Посчитаем сколько тогда осталось единиц и нулей в i -ом столбце таблицы T' :

	$supp(f_1)$	T'
0	$2^{n-3} - 1$	2^{n-3}
1	2^{n-3}	$2^{n-3} + 1$

Из таблицы видно, что для получения уравновешенного i -го столбца таблицы истинности функции f необходимо удалить из оставшихся наборов таблицы T' два набора, у которых в i -ой позиции стоит единица. Так как i — номер любого столбца, для которого справедливы выше изложенные рассуждения, делаем вывод, что у удаляемых двух наборов значения в i -ых позициях должны совпадать, другими словами, эти два набора одинаковы. Получаем противоречие с исходным выбором наборов, среди которых нет повторяющихся. Значит предположение неверно, и для любой минимальной СИ-функции от $n \geq 4$ переменных верно следующее: $wt(f) < 2^{n-1} - 2$. $\square$

3.5 Пример использования минимальных СИ-функций для исследования окрестностей заданных СИ-функций

В работе [21] было предложено использовать минимальные СИ-функции для исследования «окрестностей» заданных СИ-функций.

Как отмечалось выше, любая функция $f \in CI(n)$ может быть разложена в сумму минимальных СИ-функций с попарно непересекающимися носителями. Предположим, что уже известна некоторая функция $f \in CI(n)$, зависящая от целевого числа аргументов, но удовлетворяющая лишь части необходимых требований. Такая ситуация может возникнуть вследствие появления некоторого ранее неизвестного метода криптографического анализа, по отношению к которому функция f устойчивой не является. В этом случае предлагается рассмотреть разложение заданной функции f и разложение функции $1 \oplus f$ на минимальные СИ-функции. Очевидно, что носители минимальных СИ-функций из обоих разложений не пересекаются. Для получения функций, удовлетворяющих заданным требованиям, будем брать большую часть минимальных СИ-функций из разложения f , а из разложения $f \oplus 1$ будем брать лишь несколько функций, дополняющих уже взятые до нужного веса.

Таким образом, получающиеся функции будут являться также СИ-функциями и находиться на относительно небольшом расстоянии от заданной функции f , то есть не будут покидать определенной «окрестности» функции f .

В следующих разделах приводится пример построенных СИ-функций таким способом, в частности приводится пример применения данного подхода к функции усложнения $f_c \oplus 1$, которая используется в поточном шифре *LILI128* [30]. В результате применения метода исследования «окрестностей» была получена новая функция, которая имеет лучшие значения параметров по сравнению с параметрами исходной функции.

Также приводятся некоторые характеристики разложений СИ-функций от 4 и 5 переменных на минимальные СИ-функции

В данном разделе приведены результаты использования предложенного подхода для исследования окрестностей заданных СИ-функций.

Рассмотрим функцию $f_{10,2}^4 \in CI(10)$ из работы [19], которую далее будем обозначать через f_T :

$$f_T = 0xc53a5ac33ca5a35ca35c3ca55ac3c53a3ac5a53cc35a5ca35ca3c35aa53c3ac5a35c3ca55ac3c53a5ca3c35aa53c3ac5c53a5ac33ca5a35c3ac5a53cc35a5ca33ac5a53cc35a5ca3c53a5ac33ca5a35c5ca3c35aa53c3ac5a35c3ca55ac3c53a5ca3c35aa53c3ac53ac5a53cc35a5ca3a35c3ca55ac3c53ac53a5ac33ca5a35c$$

Функция f_T имеет следующие параметры:

$wt(f_T) = 512$	$cor(f_T) = 6$	$deg(f_T) = 3$	$nl(f_T) = 384$	$\rho(f_T) = 0$
-----------------	----------------	----------------	-----------------	-----------------

Недостатком данной функции с точки зрения применения в криптографических схемах является то, что она алгебраически вырождена ($\rho(f_T) = 0$). С помощью предложенного подхода (функции f_T и $f_T \oplus \mathbf{1}$ были разложены на 128 минимальных функций веса 4), удалось по-

лучить функцию g_T :

$$g_T = 0x3ac596c33ca5a35ca35c3ca55ac3c53a3ac5a53cc35a5ca35ca3c35aa53c3ac5a35c3ca55ac3c53a5ca3c35aa53c3ac5c53a5ac33ca5a35c3ac5a53cc35a5ca3ac5a53cc35a5ca3c53a5ac33ca5a35c5ca3c35aa53c3ac5a35c3ca55ac3c53a5ca3c35aa53c3ac53ac5a53cc35a5ca3a35c3ca55ac3c53ac53a5ac33c965ca3$$

Функция g_T имеет следующие параметры:

$wt(g_T) = 512$	$cor(g_T) = 2$	$deg(g_T) = 7$	$nl(g_T) = 360$	$\rho(g_T) = 8$
-----------------	----------------	----------------	-----------------	-----------------

Данная функция уже не является алгебраически вырожденной, а уменьшение $cor(g_T)$ и $nl(g_T)$ компенсируется существенным увеличением параметра $deg(g_T)$. При этом $dist(f_T, g_T) = 40$.

Аналогичный метод применялся к функции усложнения $f_c \oplus \mathbf{1}$,

которая используется в поточном шифре *LILI* [30].

$$f_c = 0x3cc3c33c3cc3c33c3cc3c33c3cc3c3cc3$$

$$5aa5a55a5aa5a55a5aa5a55a5aa5a5aa5$$

$$66999966669999666969969669966996$$

$$0ff0f00ff0f0ff033cccc33cc3333cc$$

$$3c3cc3c3c3c33c3c3cc33cc3c33cc33c$$

$$55aaaa55aa5555aa5a5aa5a5a5a55a5a$$

$$5aa55aa5a55aa55a666699999996666$$

$$6699669999669966696969696969696$$

Это функция от 10 переменных, имеющая следующие параметры:

$wt(f_c) = 512$	$cor(f_c) = 3$	$deg(f_c) = 6$	$nl(f_c) = 480$	$\rho(f_c) = 80$
-----------------	----------------	----------------	-----------------	------------------

В результате применения предложенного метода удалось получить функцию g_c со следующими параметрами:

$$g_c = 0x69696969969696966699669999669966$$

$$66669999999966665aa55aa5a55aa55a$$

$$5a5aa5a5996666999696696996699669$$

$$f00f0ff00ff0f00fcc3333cc33cccc33$$

$$c3c33c3c3c3cc3c3c33cc33c3cc33cc3$$

$$aa5555aa55aaaa55a5a55a5a66999966$$

$$a55a5aa55aa5a55a5aa5a55a5aa5a55a$$

$$c33c3cc33cc3c33c3cc3c33c3cc3c33c$$

$wt(g_c) = 512$	$cor(g_c) = 3$	$deg(g_c) = 6$	$nl(g_c) = 480$	$\rho(g_c) = 112$
-----------------	----------------	----------------	-----------------	-------------------

Функция g_c ни по одному параметру не хуже функции f_c , а значение параметра $\rho(g_c)$ заметно превышает $\rho(f_c)$. При этом $dist(f_c \oplus \mathbf{1}, g_c) = 288$. Таким образом, с помощью предложенных в работе подходов удалось построить функцию g_c , использование которой вместо функции f_c в шифре *LILI* позволило бы улучшить его криптографические свойства.

3.6 Разложения СИ-функций на минимальные СИ-функции

Разложить заданную СИ-функцию $f \in \mathcal{F}_n$ в сумму минимальных СИ-функций с непересекающимися носителями значит представить f в виде $f = g_1 \oplus \dots \oplus g_t$, где $g_i \in MCI(n)$ для любого i и $g_i \cdot g_j = \mathbf{0}$ при $i \neq j$.

В общем случае разложить функцию $f \in CI(n)$ на минимальные можно многими способами, то есть разложение не единственно.

Пусть

$$f = g_{1,1} \oplus g_{1,2} \oplus \dots \oplus g_{1,t_1} \oplus \dots \oplus g_{s,1} \oplus g_{s,2} \oplus \dots \oplus g_{s,t_s},$$

где $g_{i,j} \in MCI(n)$, $wt(g_{i,j}) = w_i$ и $\sum_i t_i \cdot w_i = wt(f)$ (в разложении все минимальные СИ-функции сгруппированы по весам). Тогда назовем $(w_1^{t_1}, w_2^{t_2}, \dots, w_s^{t_s})$ — весовой сигнатурой разложения функции f (далее просто сигнатурой). В общем случае для данной функции $f \in CI(n)$ может существовать множество различных сигнатур.

Заметим, что любой минимальной СИ-функции f соответствует одна сигнатура $(wt(f)^1)$ мощности 1.

3.6.1 Разложения СИ-функций от 4 переменных на минимальные СИ-функции

В этом разделе приведены сигнатуры представителей всех классов эквивалентности множества $CI(4)$. Приведены также мощности каждой из сигнатур (то есть количество различных разложений, составляющих данную сигнатуру).

f	Сигнатура	Мощность сигнату- ры	f	Сигнатура	Мощность сигнату- ры
0x0180	(2^1)	1	0x3cc3	(4^2)	3
0x03c0	(2^2)	1	0x3dda	$(2^1, 4^2)$	2
0x0660	(2^2)	1		$(2^3, 4^1)$	1
0x0690	(4^1)	1	0x3ffc	$(2^2, 4^2)$	3
0x07e0	(2^3)	1		(2^6)	1
0x0ff0	(2^4)	1		(4^3)	2
	(4^2)	1	0x6996	(2^4)	1
0x1668	(2^3)	1	0x6bd6	(2^5)	1
0x1698	$(2^1, 4^1)$	1	0x6ff6	$(2^2, 4^2)$	2
0x17e8	(2^4)	1		(2^6)	1
0x1bd8	(2^4)	1	0x6ff9	$(2^2, 4^2)$	4
0x1be4	$(2^2, 4^1)$	1		$(2^4, 4^1)$	1
	(4^2)	1		(4^3)	5
0x1ee1	$(2^2, 4^1)$	1	0x7ffe	$(2^1, 4^3)$	8
0x1ff8	$(2^1, 4^2)$	1		$(2^3, 4^2)$	6
	(2^5)	1		(2^7)	1

3.6.2 Разложения СИ-функций от 5 переменных на минимальные СИ-функции

В этом разделе приведены сигнатуры (и их мощности) тех представителей классов эквивалентности множества $CI(5)$, которые имеют порядок корреляционной иммунности равный 2, 3 и 4.

f	Сигнатура	Мощность сигнатуры
0x06609009	(4^2)	2
0x0ff0f00f	(4^4)	81
	(8^2)	4
0x1698a443	$(2^1, 4^1, 6^1)$	5
	(6^2)	1
0x17e8e817	$(4^1, 6^2)$	72
	(4^4)	53
	(8^2)	1
0x1bd8e427	$(4^1, 6^2)$	96
	(4^4)	34
0x1be4e41b	$(2^1, 4^2, 6^1)$	8
	$(2^2, 4^3)$	4
	$(2^2, 6^2)$	4
	$(2^4, 4^2)$	3
	(4^4)	4
0x1ee1e11e	$(2^2, 6^2)$	12
	$(2^4, 4^2)$	3
	(8^2)	3
0x3ddae697	$(2^1, 4^3, 6^1)$	170
	$(2^1, 6^3)$	20

	$(2^2, 4^1, 6^2)$	100
	$(2^2, 4^4)$	50
	$(2^3, 4^2, 6^1)$	90
	$(2^4, 4^3)$	5
	$(2^4, 6^2)$	5
	$(2^5, 4^1, 6^1)$	5
	$(4^2, 6^2)$	70
	(4^5)	4
0x6ff6f99f	$(2^1, 4^1, 6^3)$	1184
	$(2^1, 4^2, 6^1, 8^1)$	160
	$(2^1, 4^4, 6^1)$	2920
	$(2^1, 6^1, 8^2)$	8
	$(2^2, 4^2, 6^2)$	2956
	$(2^2, 4^3, 8^1)$	96
	$(2^2, 4^5)$	784
	$(2^3, 4^1, 6^1, 8^1)$	32
	$(2^3, 4^3, 6^1)$	1216
	$(2^3, 6^3)$	288
	$(2^4, 4^1, 6^2)$	368
	$(2^4, 4^4)$	374
	$(2^5, 4^2, 6^1)$	264
	$(2^6, 4^1, 8^1)$	8
	$(2^6, 4^3)$	32
	$(2^6, 6^2)$	36
	$(2^8, 4^2)$	2
	$(4^1, 6^2, 8^1)$	240
	$(4^2, 8^2)$	16
	$(4^3, 6^2)$	2552

	(4^6)	880
	(6^4)	112
0x3cc3c33c	$(2^2, 4^3)$	8
	$(2^4, 4^2)$	6
	(2^8)	1
	(4^4)	9
0x69969669	(4^4)	110

3.6.3 Разложение функции-константы **1** на минимальные CI-функции

Рассмотрим отдельно разложения функции-константы **1** на минимальные CI-функции.

Декомпозиция константы **1** на минимальные CI-функции позволяет построить множества $L_1, \dots, L_T$, являющиеся линейными подпространствами пространства $\mathcal{F}_n$ и состоящие из CI-функций, объединение которых дает все множество $CI(n)$.

Для функции $\mathbf{1} \in \mathcal{F}_4$ существует всего 75 разложений. Для функции $\mathbf{1} \in \mathcal{F}_5$ — 40 214 156. Далее для этих функций приведены сигнатуры и их мощности.

f	Сигнатура	Мощность сигнату- ры	f	Сигнатура	Мощность сигнату- ры
0xffff	$(2^2, 4^3)$	32	0xffffffff	$(2^4, 4^4, 8^1)$	44160
	$(2^4, 4^2)$	12		$(2^4, 4^6)$	264340
	(2^8)	1		$(2^4, 6^4)$	145080

	(4^4)	30		$(2^5, 4^1, 6^3)$	238080
0xffffffff	$(2^1, 4^1, 6^3, 8^1)$	355200		$(2^5, 4^2, 6^1, 8^1)$	28800
	$(2^1, 4^2, 6^1, 8^2)$	33600		$(2^5, 4^4, 6^1)$	506400
	$(2^1, 4^3, 6^3)$	7948800		$(2^5, 6^1, 8^2)$	480
	$(2^1, 4^4, 6^1, 8^1)$	456960		$(2^6, 4^2, 6^2)$	199440
	$(2^1, 4^6, 6^1)$	3302880		$(2^6, 4^3, 8^1)$	7200
	$(2^1, 6^5)$	517632		$(2^6, 4^5)$	56064
	$(2^{10}, 4^3)$	720		$(2^7, 4^1, 6^1, 8^1)$	2880
	$(2^{10}, 6^2)$	432		$(2^7, 4^3, 6^1)$	55680
	$(2^{12}, 4^2)$	100		$(2^7, 6^3)$	6400
	$(2^2, 4^1, 6^4)$	2077440		$(2^8, 4^1, 6^2)$	8640
	$(2^2, 4^2, 6^2, 8^1)$	504960		$(2^8, 4^4)$	8010
	$(2^2, 4^3, 8^2)$	4960		$(2^8, 8^2)$	80
	$(2^2, 4^4, 6^2)$	6860880		$(2^9, 4^2, 6^1)$	4320
	$(2^2, 4^5, 8^1)$	114240		(2^{16})	1
	$(2^2, 4^7)$	596400		$(4^1, 6^2, 8^2)$	22080
	$(2^2, 6^2, 8^2)$	12000		$(4^2, 6^4)$	3461880
	$(2^3, 4^1, 6^1, 8^2)$	3840		$(4^3, 6^2, 8^1)$	465600
	$(2^3, 4^2, 6^3)$	2896000		$(4^4, 8^2)$	17200
	$(2^3, 4^3, 6^1, 8^1)$	252480		$(4^5, 6^2)$	4183872
	$(2^3, 4^5, 6^1)$	2192640		$(4^6, 8^1)$	22080
	$(2^3, 6^3, 8^1)$	42240		(4^8)	365065
	$(2^4, 4^1, 6^2, 8^1)$	72960		$(6^4, 8^1)$	42240
	$(2^4, 4^2, 8^2)$	2160		(8^4)	400
	$(2^4, 4^3, 6^2)$	1808160			

Глава 4

Асимптотические оценки мощностей множеств $CI(n, w)$ и $BCI(n, w)$

4.1 Оценка мощности множества $CI(n, w)$

Докажем утверждение об асимптотическом поведении мощности множества $CI(n, w)$.

Теорема 12. Пусть w — четное фиксированное число, $w > 1$. Справедливо соотношение:

$$\lim_{n \rightarrow \infty} \frac{|CI(n, w)|}{\frac{\binom{w}{w/2}^n}{w!}} = 1.$$

Доказательство. Посчитаем количество $(w \times n)$ -матриц, у которых каждый столбец является уравновешенным. Обозначим множество таких таблиц через S . Число уравновешенных столбцов длины w равно $\binom{w}{w/2}$. Тогда $|S| = \left(\binom{w}{w/2}\right)^n$.

Оценим число таблиц из множества S , которые имеют одинаковые строки. Обозначим множество таких таблиц через T . Рассмотрим два случая:

1. $w = 2$

В этом случае множество таблиц из множества S с одинаковыми строками пусто: $T = \emptyset$.

2. $w > 2$

Число уравновешенных столбцов длины w с одинаковыми элементами на позициях i и j равно $2 \cdot \binom{w-2}{\frac{w}{2}}$. Тогда число таблиц с одинаковыми строками i и j равно $(2 \cdot \binom{w-2}{\frac{w}{2}})^n$. Откуда получаем оценку мощности множества T :

$$|T| \leq \sum_{(i,j), 1 \leq i < j \leq w} \left(2 \cdot \binom{w-2}{\frac{w}{2}} \right)^n = \frac{w \cdot (w-1)}{2} \cdot \left(\binom{w-2}{\frac{w}{2}} \right)^n \cdot 2^n.$$

Оценим долю таблиц из множества T среди всех таблиц из множества S и обозначим полученное значение через A :

$$\begin{aligned} A = \frac{|T|}{|S|} &\leq \frac{\frac{w \cdot (w-1)}{2} \cdot \left(\binom{w-2}{\frac{w}{2}} \right)^n}{\left(\binom{w}{\frac{w}{2}} \right)^n} \cdot 2^n = \\ &= w \cdot (w-1) \cdot 2^{n-1} \cdot \left(\frac{(w-2)! \cdot \frac{w}{2}! \cdot \frac{w}{2}!}{\frac{w}{2}! \cdot (\frac{w}{2}-2)! \cdot w!} \right)^n = \\ &= w \cdot (w-1) \cdot 2^{n-1} \cdot \left(\frac{\left(\frac{w}{2} - 1 \right) \cdot \frac{w}{2}}{w \cdot (w-1)} \right)^n = \\ &= \frac{w \cdot (w-1)}{2^{n+1}} \cdot \left(1 - \frac{1}{w-1} \right)^n. \end{aligned}$$

При фиксированном $w > 2$ и n стремящемся к бесконечности

доля таблиц с одинаковыми строками стремится к 0:

$$\lim_{n \rightarrow \infty} A = 0.$$

Обозначим M — подмножество S , состоящее из таблиц без повторяющихся строк, то есть $M = S \setminus T$, $|M| = |S| - |T|$. В случае $w = 2$ множество M совпадает с множеством S . Тогда

$$\lim_{n \rightarrow \infty} \frac{|M|}{|S|} = \lim_{n \rightarrow \infty} \frac{|S| - |T|}{|S|} = \lim_{n \rightarrow \infty} \left(1 - \frac{|T|}{|S|}\right) = 1.$$

Согласно определению таблицы истинности и Следствию 1, множество M является множеством таблиц истинности CI-функций. Разные таблицы из множества M могут являться таблицей истинности одной и той же функции $f \in CI(n, w)$, если перестановкой строк переводятся друг в друга, то есть $w!$ таблиц дают одну и ту же функцию. Тогда

$$|CI(n, w)| = \frac{|M|}{w!},$$

$$\lim_{n \rightarrow \infty} \frac{|CI(n, w)|}{\frac{\binom{w}{w/2}^n}{w!}} = 1.$$

□

4.2 Оценка мощности множества $BCI(n, w)$

Докажем утверждение об асимптотическом поведении мощности множества $BCI(n, w)$.

Теорема 13. Пусть w — четное фиксированное число, $w > 2$. Спра-

ведливо соотношение:

$$\lim_{n \rightarrow \infty} \frac{|BCI(n, w)|}{\frac{\left(\frac{w}{2}\right)^n}{w!}} = 1.$$

Доказательство. Обозначим множество таблиц с n уравновешенными столбцами и w строками через S . Аналогично доказательству теоремы 12

$$|S| = \left(\frac{w}{2}\right)^n.$$

Согласно определению, множество $BCI(n, w)$ состоит из CI-функций от n переменных веса w , ни в одном разложении которых на минимальные CI-функции нет функций из множества $Mir(n)$ (см. [1]). Значит, в таблицах истинности CI-функций из множества $BCI(n, w)$ нет взаимнообратных наборов.

Оценим число таблиц из множества S , строки которых являются взаимнообратными наборами. Обозначим множество таких таблиц через D . Число уравновешенных столбцов длины $w > 2$ с противоположными элементами на позициях i и j равно $2 \cdot \left(\frac{w-2}{2}\right)$. Тогда число таблиц с противоположными строками i и j равно $\left(2 \cdot \left(\frac{w-2}{2}\right)\right)^n$. Откуда получаем оценку мощности множества D :

$$|D| \leq \sum_{(i,j), 1 \leq i < j \leq w} \left(2 \cdot \left(\frac{w-2}{2}\right)\right)^n = \frac{w \cdot (w-1)}{2} \cdot \left(\frac{w-2}{2}\right)^n \cdot 2^n.$$

Оценим долю таблиц, строки которых являются взаимнообрат-

ными, среди всех таблиц из множества S :

$$\begin{aligned}
B &= \frac{|D|}{|S|} \leq \frac{\frac{w \cdot (w-1)}{2} \cdot \left(\frac{w-2}{2}\right)^n}{\left(\frac{w}{2}\right)^n} \cdot 2^n = \\
&= w \cdot (w-1) \cdot 2^{n-1} \cdot \left(\frac{(w-2)! \cdot \frac{w}{2}! \cdot \frac{w}{2}!}{\left(\frac{w}{2}-1\right)! \cdot \left(\frac{w}{2}-1\right)! \cdot w!} \right)^n = \\
&= \frac{w \cdot (w-1)}{2} \cdot \left(\frac{1 + \frac{1}{w-1}}{2} \right)^n.
\end{aligned}$$

При $w > 2$ верна следующая цепочка неравенств:

$$\begin{aligned}
0 &< \frac{1}{w-1} < 1, \\
1 &< 1 + \frac{1}{w-1} < 2, \\
\frac{1}{2} &< \frac{1 + \frac{1}{w-1}}{2} < 1.
\end{aligned}$$

Следовательно, при фиксированном $w > 2$ и n стремящемся к бесконечности доля таблиц с строками, которые являются взаимнообратными наборами, стремится к 0:

$$\lim_{n \rightarrow \infty} B = 0.$$

Обозначим T — подмножество S , состоящее из таблиц с одинаковыми строками, N — подмножество S , состоящее из таблиц без повторяющихся строк и без строк, являющихся взаимнообратными наборами. Тогда множество N является множеством таблиц истинности из множества $BCI(n, w)$. Тогда

$$N = S \setminus (D \cup T), |N| = |S| - |D \cup T| = |S| - (|D| + |T|) + |D \cap T|.$$

Так как

$$\lim_{n \rightarrow \infty} \frac{|D|}{|S|} = 0, \lim_{n \rightarrow \infty} \frac{|T|}{|S|} = 0,$$

то

$$\lim_{n \rightarrow \infty} \frac{|D| + |T|}{|S|} = 0,$$

$$\lim_{n \rightarrow \infty} \frac{|D \cap T|}{|S|} = 0.$$

Тогда

$$\lim_{n \rightarrow \infty} \frac{|N|}{|S|} = 1.$$

Разные таблицы из множества N могут являться таблицей истинности одной и той же функции $f \in BCI(n, w)$, если перестановкой строк переводятся друг в друга, то есть $w!$ таблиц дают одну и ту же функцию. Тогда

$$|BCI(n, w)| = \frac{|N|}{w!},$$

$$\lim_{n \rightarrow \infty} \frac{|BCI(n, w)|}{\frac{\left(\frac{w}{2}\right)^n}{w!}} = 1.$$

□

4.3 Верхняя оценка мощности множества

$$CI(n, w)$$

Утверждение 4. Пусть w — четное фиксированное число, $w \geq 2$.
Справедлива следующая верхняя оценка:

$$|CI(n, w)| \leq \frac{\binom{w}{w/2}^n}{w!}.$$

При $w = 2$ верхняя оценка достижима.

Доказательство. Из доказательства Теоремы 12 справедливы следующие равенства:

$$|M| = |S| - |T|,$$

$$|CI(n, w)| = \frac{|M|}{w!}.$$

Пусть $w > 2$. Тогда:

$$|M| < |S| = \binom{w}{w/2}^n,$$

$$|CI(n, w)| < \frac{\binom{w}{w/2}^n}{w!}.$$

Пусть $w = 2$. Тогда:

$$|T| = 0,$$

$$|M| = |S| = \binom{w}{w/2}^n,$$

$$|CI(n, w)| = \frac{\binom{w}{w/2}^n}{w!}.$$

□

Рассмотрим таблицы ниже. Во втором столбце таблиц указаны верхние оценки мощности множества $CI(n, w)$ при различных параметрах согласно Утверждению 4. Обозначим значение верхней оценки через $S'(n, w) = \frac{\binom{w}{w/2}^n}{w!}$. В третьем столбце указаны мощности множества $CI(n, w)$ при различных параметрах.

w	$S'(4, w)$	$ CI(4, w) $
2	8	8
4	54	52
6	222	152
8	595	222

w	$S'(5, w)$	$ CI(5, w) $
2	16	16
4	324	320
6	4444	3824
8	41684	27640
10	280 053	123 600
12	1 406 122	353 120
14	5 461 702	657 520
16	16 876 141	807 980

w	$S'(6, w)$	$ CI(6, w) $
2	32	32
4	1944	1936
6	88 889	83 680
8	2 917 881	2 452 080
10	70 573 265	49 585 440
12	1 299 256 395	712 645 616
14	18 744 563 130	7 472 934 880
16	217 195 932 415	58 431 976 800

Обозначим через $A'(n, w)$ следующее значение:

$$A'(n, w) = \frac{\frac{\binom{w}{w/2}^n}{w!} - |CI(n, w)|}{|CI(n, w)|} = \frac{S'(n, w) - |CI(n, w)|}{|CI(n, w)|}.$$

При анализе формулы из Теоремы 12 при фиксированных параметрах с использованием данных из предыдущих таблиц был получен следующий результат в процентах:

w	$A'(4, w)$	$A'(5, w)$	$A'(6, w)$
2	0	0	0
4	3.85	1.25	0.41
6	46	16.21	6.22
8	168	50.8	19
10		126.58	42.3
12			82.3
14			150.8

Заключение

В настоящей работе получены следующие новые результаты.

1. Предложен метод построения СИ-функций и минимальных СИ-функций, основанный на комбинации рекурсивного и переборного методов. На первом этапе с помощью перебора строятся минимальные СИ-функции от малого числа переменных. Примеры таких функций от 4, 5, 6 переменных получены с помощью вычислительной техники и представлены в работе. Далее для построения минимальных СИ-функций от большего числа переменных в работе предложено преобразование, которое позволяет быстро наращивать число переменных. Доказано, что применение такого преобразования к минимальной СИ-функции или к СИ-функции позволяет построить функцию, которая также является минимальной СИ-функцией или СИ-функцией соответственно, но уже зависит от большего числа аргументов. С помощью построенных таким образом минимальных СИ-функций от большого числа переменных реализуется второй этап метода: СИ-функции от заданного числа переменных строятся как сумма минимальных СИ-функций от этого же числа переменных с непересекающимися носителями.
2. Представлены классификации минимальных СИ-функций от 4, 5, 6 переменных. Посчитаны мощности классов, а для каждого представителя класса посчитаны и приведены в таблицах такие значения параметров функции, как вес, степень, нелинейность, порядок корреляционной-иммунности и невырожденность.

3. Построены устойчивые функции от 7, 8, 9, 10, 11 переменных с помощью предложенного метода.
4. Доказан критерий равенства СИ-функций, полученных с помощью введенного преобразования для наращивания числа переменных. Данный критерий используется в ходе доказательства верхней и нижней оценки мощности множеств СИ-функций, получаемых подобным образом. Теоретические оценки подтверждены практическими результатами: в работе представлено сравнение теоретических значений мощностей полученных множеств с реальными значениями для СИ-функций от 4, 5 и 6 переменных. Практические оценки получены с помощью вычислительной техники.
5. Понижена верхняя оценка веса минимальных СИ-функций. Доказано, что любая минимальная СИ-функция существенно зависит от всех своих переменных. Доказан критерий минимальности и сформулировано достаточное условие существования минимальных СИ-функций.
6. Получены асимптотические оценки множеств $CI(n, w)$ и $BCI(n, w)$. Получена верхняя оценка мощности множества $CI(n, w)$.

Полученные результаты могут быть полезны специалистам Московского государственного университета им. М. В. Ломоносова, в том числе — специалистам Центра проблем информационной безопасности (ИПИБ) факультета ВМК, специалистам Института прикладной математики и кибернетики им. М. В. Келдыша, Института математики им. С. Л. Соболева СО РАН, Института криптографии, свя-

зи и информатики Академии ФСБ России. Кроме того, результаты диссертации могут быть использованы при подготовке лекционных курсов по тематике синтеза и анализа криптографических функций.

Литература

- [1] Алексеев Е.К. «О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций» Дискретная математика. 2010. Т. 22. С. 110 – 126.
- [2] Алексеев Е.К., «Об атаке на фильтрующий генератор с функцией усложнения близкой к алгебраически вырожденной», Сборник статей молодых ученых факультета ВМК МГУ, 2011, №8, 19-32.
- [3] Алексеев Е.К. «О некоторых мерах нелинейности булевых функций», ПДМ, 2011, №2, 5–16.
- [4] Алексеев Е.К., Карелина Е.К. «Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных», Дискретная математика, 2015, Т. 27.
- [5] Ботев А.А. «Новые соотношения между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций», Материалы V научной школы по дискретной математике и ее приложениям, Москва, 12-17 ноября 2001 г. М.: издательство центра прикладных исследований при механико-математическом факультете МГУ, 2002 г., С. 20-26.
- [6] Ботев А.А. «О взаимосвязи корреляционной иммунности и нелинейности для неуравновешенных булевых функций», Материалы XII международной школы-семинара «Синтез и сложность управляющих систем».

- [7] Ботев А.А. «О соотношении между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций», Математические вопросы кибернетики, вып. 11, М., Физматлит, 2002, С. 149-162.
- [8] Ботев А.А. «Об алгебраической иммунности одной рекурсивно заданной последовательности корреляционно-иммунных функций», Материалы XV международной школы-семинара «Синтез и сложность управляющих систем», Новосибирск, 18-23 октября 2004 г., Новосибирск: издательство института математики СО РАН, 2004 г., С. 8-12.
- [9] Ботев А.А. «Об алгебраической иммунности рекурсивных конструкций нелинейных фильтров», Материалы III общероссийской конференции «Математика и безопасность информационных технологий», (Мабит-04), М.: МЦНМО, 2005, С. 131-135.
- [10] Ботев А.А. «Об алгебраической иммунности новых конструкций функций с высокой нелинейностью», Дискретные модели в теории управляющих систем: VI Международная конференция: Москва, 7-11 декабря, 2004 г., Труды, М.: Издательский отдел Факультета ВМК МГУ имени М.В. Ломоносова, 2004, С. 227-231.
- [11] Денисов О.В. «Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций», Дискретная математика, том 3, вып. 2, 1991, С. 25-46.

- [12] Денисов О.В. «Локальная предельная теорема для распределения части спектра случайной двоичной функции», Дискретн. математика, том 12, вып. 1, 2000, С. 82-95.
- [13] Карелина Е.К. «Об одном методе синтеза корреляционно-иммунных булевых функций», Дискретная математика, 2018, Т. 30.
- [14] Карелина Е.К. «Мощностные оценки множества корреляционно-иммунных булевых функций», Дискретная математика, 2021, Т. 33.
- [15] Карелина Е.К. «Мощностные оценки множества корреляционно-иммунных функций, получаемого с помощью отображения AC^w », International Journal of Open Information Technologies, 2022, Т. 10.
- [16] Кущинская Л.А. «Исследование границ применимости некоторых методов криптографического анализа потоковых шифров, построенных на основе регистров сдвига», Дипломная работа. МГУ, Факультет ВМК, 34 с., 2015.
- [17] Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В. «Булевы функции в теории кодирования и криптологии», Москва: Ленанд, 2021, С. 576.
- [18] Лупанов О.Б. «Об одном подходе к синтезу управляющих систем — принципе локального кодирования», Проблемы кибернетики, вып. 14, М.: Наука, 1965, с. 31-110.

- [19] Таранников Ю.В. «О корреляционно-иммунных и устойчивых булевых функциях», Математические вопросы кибернетики, 2002. Т. 11. С. 91 — 148.
- [20] Таранников Ю.В. «Комбинаторные свойства дискретных структур и приложения к криптологии», М.: МЦНМО, 2011, С. 152.
- [21] Alekseev E.K., Karelina E.K., Logachev O.A. «On construction of correlation-immune functions via minimal functions», Математические вопросы криптографии, 2018, Т. 9, No 2 С. 7 — 22.
- [22] Bernasconi A. «Harmonic Analysis and Boolean Function Complexity», CALCOLO 35, 1998, pp. 149-186.
- [23] Braeken A., Borissov Y., Nikova S., Preneel B. «Classification of Boolean Functions of 6 Variables or Less with Respect to Cryptographic Properties», Cryptology ePrint Archive, Report 2004/248.
- [24] Brier E., Langevin P. «Classification of Boolean Cubic Forms of Nine Variables», 2003, IEEE Information Theory Workshop (ITW 2003), IEEE Press, pp. 179-182, 2002.
- [25] Camion P., Carlet C., Charpin P., Sendrier N. «On correlation-immune functions», In Proceedings of CRYPTO'91, LNCS №576, Springer, Berlin, Heidelberg, 1992, pp. 91-148.
- [26] Carlet C. «Boolean Functions for Cryptography and Coding Theory», Cambridge University Press, New York, 2020, pp. 562.
- [27] Carlet C., Chen X. «Constructing Low-Weight d^{th} -order Correlation-Immune Boolean Functions Through the Fourier-

- Hadamard Transform», IEEE Trans.on Inform. Theory, v.64, №4, 2018, pp. 2969-2978.
- [28] Courtois N., Meier W. «Algebraic attacks on stream ciphers with linear feedback», Proceedings of EUROCRYPT 2003, LNCS, vol 2656, pp. 346–359.
 - [29] Cusick T. W., Stanica P. «Cryptographic Boolean Functions and Applications», Elsevier-Academic Press, 2009, pp. 232.
 - [30] Dawson E., Clark A., Golich J., Millan W., Penna L., Simpson L. «The LILI-128 keystream generator». Proc. of first NESSIE workshop, pp. 1-14, 2000.
 - [31] Harrison M.A. «On the Classification of Boolean Functions by the General Linear and Affine Group», Journal of the Society for industrial and applied mathematics, Vol.12, pp.284-299, 1964.
 - [32] Hedayat A.S., Sloane N.J.A., Stufken J. «Orthogonal arrays. Theory and Applications. Springer series in statistics», Berlin, Heidelberg, Springer-Verlag, 1999, pp. 416.
 - [33] Maiorana J. «A Classification of the Cosets of the Reed-Muller Code $R(1,6)$ », Mathematics of Computation, vol.57, No.195, July 1991, pp.403-414.
 - [34] Matsui M. «Linear Cryptanalysis Method for DES Cipher», Advanced in Cryptology – EUROCRYPT’93. Lect. Notes in Comp. Sci., Springer, 1994. V. 765. P. 386-397.
 - [35] Meier W., Staffelbach O. «Nonlinearity criteria for cryptographic functions», Springer Verlag. 1989. Vol. EUROCRYPT’89.

- [36] Meier W., Staffelbach O. «Fast correlation attacks on certain stream ciphers», *Journal of Cryptology*, vol. 1, 1989, pp. 159-176.
- [37] Menezes A., van Oorschot P., Vanstone S. «Handbook of Applied Cryptography», CRC Press, 1996, pp. 816.
- [38] Pasalic E., Johansson T. «Further results on the relation between nonlinearity and resiliency for Boolean Function», *IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science*, V. 1746., 1999, pp. 35-44.
- [39] Siegenthaler T. «Correlation-immunity of nonlinear combining functions for cryptographic applications», *IEEE Trans. On Information Theory*, vol. IT-30, №5, 1984, pp. 776-780.
- [40] Siegenthaler T. «Decrypting a Class of Stream Cipher Using Ciphertext Only», *IEEE Trans. On Computers*, vol. c-34, 1985.
- [41] Siegenthaler T. «Design of Combiners to Prevent Divide and Conquer Attacks», In *Proceedings of CRYPTO'85, LNCS №218*, Springer-Verlag, 1986, pp. 273-279.
- [42] Siegenthaler T. «Cryptanalysis of Nonlinear Filtered ML-Sequences», In *Proceedings of EUROCRYPT'86, LNCS №219*, Springer-Verlag, pp. 103-110.
- [43] Tarannikov Yu, Korolev P., Botev A. «Autocorrelation Coefficients and Correlation Immunity of Boolean Functions», *Proceedings of Asiacrypt*, 2001, T. 2248, C. 460 – 479.
- [44] Wu C.-K., Feng D. «Boolean Functions and Their Applications in Cryptography», Springer-Verlag, Berlin, Heidelberg, 2016, pp. 256.

- [45] Wu C.-K., Dawson E. «Construction of Correlation Immune Boolean Functions», *Australasian J. of Combinatorics*, 21, 2000, pp. 141-166.

Приложение

4.4 Классификация СИ-функций от 4 переменных

В следующей таблице приведена полная классификация СИ-функций от 4 переменных.

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$	$\rho(f)$	$\delta(f)$	$ f^{\mathcal{D}_n} $
0x0000	0	0	0	4	0	0	1
0x0180	2	3	2	1	0	0	8
0x03c0	4	2	4	1	0	0	16
0x0660	4	2	4	1	0	0	12
0x0690	4	2	4	1	0	0	24
0x07e0	6	3	2	1	0	0	48
0x1668	6	3	2	1	0	0	8
0x1698	6	3	4	1	2	2	96
0x0ff0	8	1	0	1	0	0	12
0x17e8	8	2	4	1	0	0	32
0x1bd8	8	2	4	1	0	0	24
0x1be4	8	2	4	1	0	0	96
0x1ee1	8	2	4	1	0	0	48
0x3cc3	8	1	0	2	0	0	8
0x6996	8	1	0	3	0	0	2
0x1ff8	10	3	2	1	0	0	48
0x3dda	10	3	4	1	2	2	96
0x6bd6	10	3	2	1	0	0	8

0x6ff6	12	2	4	1	0	0	12
0x3ffc	12	2	4	1	0	0	16
0x6ff9	12	2	4	1	0	0	24
0x7ffe	14	3	2	1	0	0	8
0xffff	16	0	0	4	0	0	1

4.5 Все минимальные СИ-функций от 4 переменных

Далее представлены все минимальные СИ-функции от 4 переменных:

f	$wt(f)$	$deg(f)$	$nl(f)$	$cor(f)$	$\rho(f)$	$\delta(f)$
0x0180	2	3	2	1	0	0
0x0240	2	3	2	1	0	0
0x0420	2	3	2	1	0	0
0x0810	2	3	2	1	0	0
0x1008	2	3	2	1	0	0
0x2004	2	3	2	1	0	0
0x4002	2	3	2	1	0	0
0x8001	2	3	2	1	0	0
0x0690	4	2	4	1	0	0
0x0960	4	2	4	1	0	0
0x1284	4	2	4	1	0	0
0x1482	4	2	4	1	0	0

0x1824	4	2	4	1	0	0
0x1842	4	2	4	1	0	0
0x1881	4	2	4	1	0	0
0x2148	4	2	4	1	0	0
0x2418	4	2	4	1	0	0
0x2442	4	2	4	1	0	0
0x2481	4	2	4	1	0	0
0x2841	4	2	4	1	0	0
0x4128	4	2	4	1	0	0
0x4218	4	2	4	1	0	0
0x4224	4	2	4	1	0	0
0x4281	4	2	4	1	0	0
0x4821	4	2	4	1	0	0
0x6009	4	2	4	1	0	0
0x8118	4	2	4	1	0	0
0x8124	4	2	4	1	0	0
0x8142	4	2	4	1	0	0
0x8214	4	2	4	1	0	0
0x8412	4	2	4	1	0	0
0x9006	4	2	4	1	0	0

4.6 Мощности множеств СИ-функций, полученных с помощью отображения $AC_{v,i}^w$

В данном разделе приводятся результаты применения отображения $AC_{v,i}^w$ к СИ-функциями и минимальным СИ-функциям от 4, 5, 6 переменных.

В таблицах записано следующее. В первом столбце указывается значение функции, к которой применялось отображение $AC_{v,i}^w$, во втором столбце указывается вес рассматриваемой функции, в третьем столбце записывается количество различных функций, полученных после применения отображения $AC_{v,i}^w$ к рассматриваемой функции из первого столбца, в четвертом столбце указано общее число функций рассматриваемого веса, применение к которым отображения $AC_{v,i}^w$ дает столько же различных функций, как и к рассматриваемой.

4.6.1 Результаты для СИ-функций и минимальных СИ-функций от 4 переменных

Будем рассматривать указанные функции по весам.

1. Рассмотрим функции веса 2. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(2)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_2 : wt(v) = 1\},$$

$$2 \leq |M| \leq 6$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x0420	2	5	1
0x0180	2	6	7

2. Рассмотрим функции веса 4. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(4)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_4 : wt(v) = 2\},$$

$$8 \leq |M| \leq 26$$

Полученные результаты для минимальных CI-функций:

f	$wt(f)$	$ M $	—
0x2841	4	24	2
0x0690	4	25	14
0x1284	4	26	8

Полученные результаты для CI-функций:

f	$wt(f)$	$ M $	—
0x0c30	4	22	2
0x03c0	4	23	14
0x0660	4	24	3
0x0690	4	25	20
0x1284	4	26	13

3. Рассмотрим функции веса 6. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(6)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_6 : wt(v) = 3\},$$

$$32 \leq |M| \leq 96$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x2a54	6	86	1
0x07e0	6	87	11
0x25a4	6	89	5
0x0bd0	6	90	32
0x2c61	6	92	2
0x1698	6	93	38
0x19a4	6	94	59
0x4992	6	95	4

4. Рассмотрим функции веса 8. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(8)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_8 : wt(v) = 4\},$$

$$124 \leq |M| \leq 346$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x0ff0	8	303	4
0x9999	8	304	2
0x33cc	8	315	5
0xc3c3	8	316	1
0x17e8	8	328	12
0x2e74	8	330	2
0x1bd8	8	334	38
0x1ee1	8	336	12
0x1be4	8	337	108
0x2dd2	8	339	36
0x6996	8	340	2

5. Рассмотрим функции веса 10. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(10)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_{10} : wt(v) = 5\},$$

$$472 \leq |M| \leq 1256$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x1ff8	10	1204	5
0x57ea	10	1208	7
0x2ff4	10	1216	13
0x37ec	10	1220	23
0xe997	10	1226	1
0x79cb	10	1228	2
0x3dda	10	1232	36
0x97e9	10	1235	2
0x3de6	10	1236	58
0x799e	10	1238	1
0x6db6	10	1240	1
0x6bd6	10	1241	3

6. Рассмотрим функции веса 12. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(12)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_{12} : wt(v) = 6\},$$

$$1785 \leq |M| \leq 4616$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x3ffc	12	4463	2
0xdbdb	12	4492	2
0x5ffa	12	4493	8
0xbbdd	12	4508	4
0x6ff6	12	4524	3
0x6ff9	12	4525	4
0x9ff9	12	4528	2
0xf99f	12	4532	1
0x7bde	12	4540	14
0x7ebd	12	4541	2
0xd7eb	12	4544	2
0xb7ed	12	4556	8

7. Рассмотрим функции веса 14. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(14)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_{14} : wt(v) = 7\},$$

$$6736 \leq |M| \leq 17156$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x7ffe	14	16555	1
0xbffd	14	16727	2
0xeff7	14	16784	1
0xfbdf	14	16840	1
0xdffb	14	16844	3

8. Рассмотрим функции веса 16. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(16)}(f, v, i), f \in CI(4), i \in \{1 \dots 5\}, v \in V_{16} : wt(v) = 8\},$$

$$25484 \leq |M| \leq 64346$$

Полученные результаты:

0xffff	16	61932	1
--------	----	-------	---

4.6.2 Результаты для минимальных CI-функций от 5 переменных

Будем рассматривать указанные функции по весам.

1. Рассмотрим функции веса 2. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(2)}(f, v, i), f \in MCI(5), i \in \{1 \dots 6\}, v \in V_2 : wt(v) = 1\},$$

$$2 \leq |M| \leq 7$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x00200400	2	6	1
0x00018000	2	7	15

2. Рассмотрим функции веса 4. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(4)}(f, v, i), f \in MCI(5), i \in \{1 \dots 6\}, v \in V_4 : wt(v) = 2\},$$

$$8 \leq |M| \leq 31$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x00069000	4	30	50
0x00128400	4	31	150

3. Рассмотрим функции веса 6. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(6)}(f, v, i), f \in MCI(5), i \in \{1 \dots 6\}, v \in V_6 : wt(v) = 3\},$$

$$32 \leq |M| \leq 115$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x01186008	6	112	24
0x0118a004	6	113	146
0x01244820	6	114	322
0x01188240	6	115	372

4. Рассмотрим функции веса 8. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(8)}(f, v, i), f \in MCI(5), i \in \{1 \dots 6\}, v \in V_8 : wt(v) = 4\},$$

$$124 \leq |M| \leq 415$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x01686801	8	411	8
0x14422881	8	412	4
0x02949402	8	413	32
0x04929204	8	414	64
0x09249042	8	415	52

4.6.3 Результаты для минимальных CI-функций от 6 переменных

Будем рассматривать указанные функции по весам.

1. Рассмотрим функции веса 2. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(2)}(f, v, i), f \in MCI(6), i \in \{1 \dots 7\}, v \in V_2 : wt(v) = 1\},$$

$$2 \leq |M| \leq 8$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x0000 0400 0020 0000	2	7	1
0x8000 0000 0000 0001	2	8	31

2. Рассмотрим функции веса 4. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(4)}(f, v, i), f \in MCI(6), i \in \{1 \dots 7\}, v \in V_4 : wt(v) = 2\},$$

$$8 \leq |M| \leq 36$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x0020 0400 0020 0400	4	32	2
0xc000 0000 0000 0003	4	33	94
0x0000 2400 0024 0000	4	34	3
0x6000 0000 0000 0009	4	35	188
0x9000 0000 0000 0009	4	36	1649

3. Рассмотрим функции веса 6. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(6)}(f, v, i), f \in MCI(6), i \in \{1 \dots 7\}, v \in V_6 : wt(v) = 3\},$$

$$32 \leq |M| \leq 136$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0xe000 0000 0000 0007	6	125	80
0xd000 0000 0000 000b	6	128	400
0xa400 0000 0000 0025	6	130	36
0xc200 0000 0000 0043	6	131	1996
0xa400 0000 0000 0043	6	132	9795
0x6080 0000 0000 0403	6	133	26118
0x9200 0000 0000 0049	6	134	45255

4. Рассмотрим функции веса 8. По теоремам 11 и 10 получаем следующие оценки:

$$M = \{g = AC^{(8)}(f, v, i), f \in MCI(6), i \in \{1 \dots 7\}, v \in V_8 : wt(v) = 4\},$$

$$124 \leq |M| \leq 484$$

Полученные результаты:

f	$wt(f)$	$ M $	—
0x0420 0420 0420 0420	8	441	2
0xf000 0000 0000 000f	8	442	38
0x0030 0c00 0030 0c00	8	453	1
0xcc00 0000 0000 0033	8	454	79
0xe800 0000 0000 0017	8	466	32
0x2400 2400 0024 0024	8	467	10
0x3c00 0000 0000 00c3	8	468	376
0xc300 0000 0000 00c3	8	469	1294
0xe080 0000 0000 0107	8	472	256
0x7000 0800 0080 0007	8	474	20
0xe400 0000 0000 0027	8	475	5532
0x8880 1000 1000 0007	8	477	186
0xd200 0000 0000 0087	8	478	34754
0xc820 0000 0000 1007	8	479	42872
0xc210 0000 0000 8007	8	480	106942
0x9840 0000 0000 2007	8	481	339433
0x9420 0000 0000 8007	8	482	572955

0x6810 0000 0000 0843	8	483	846923
0x6810 0000 0000 0429	8	484	500375