Мощностные оценки множества корреляционно-иммунных функций, получаемого с помощью отображения AC^w

Е. К. Карелина

***Аннотация* — В одной из работ, посвященных изучению корреляционно-иммунных функций, было введено отображение AC^w. Отображение AC^w позволяет быстро наращивать число переменных функции. Его использование легло в основу рекурсивного метода синтеза корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций. Однако применение отображения к функции со всеми возможными параметрами позволяет получить в том числе и равные между собой функции. В настоящей работе приводится критерий равенства двух функций, получаемых с помощью отображения AC^w. В работе доказываются нижняя и верхняя оценки мощности множества корреляционно-иммунных функций, которое получается при применении данного отображения к исходной функции. При доказательстве этих оценок используется вышеупомянутый критерий равенства функций. В работе приведено несколько примеров корреляционно-иммунных функций различных весов от малого числа переменных, к которым было применено отображение AC^w. Также в работе приводятся значения мощностей соответствующих множеств, получаемых после применения этого отображения к заданным корреляционно-иммунным функциям. Данные результаты были получены с помощью вычислительной техники и подтверждают доказанные верхние и нижние оценки для рассматриваемых множеств функций.**

***Ключевые слова* — корреляционно-иммунные функции, построение корреляционно-иммунных функций, оценки мощности.**

I. Введение

Понятие «корреляционно-иммунная функция» (далее, CI-функция) было введено Т. Зигенталером в одной из своих работ. Использование таких функций при синтезе комбинирующего и фильтрующего генераторов позволяет противостоять корреляционной атаке. Поэтому существенный интерес представляет задача построения CI-функций от большого числа переменных.

На сегодняшний день можно выделить два подхода к построению CI-функций. Первый подход объединяет методы решения задачи, имеющие рекурсивный характер. Каждая новая функция является результатом применения определенных преобразований к функциям от меньшего числа переменных [1]. Второй подход заключается в использовании минимальных CI-функций. Данное понятие было введено в работе [2], и было доказано, что любая CI-функция раскладывается в сумму минимальных CI-функций с непересекающимися носителями. Именно это свойство легло в основу альтернативного метода построения CI-функций: CI-функция с целевыми параметрами ищется среди функций, построенных с помощью специальным образом подобранного множества минимальных CI-функций [3]. Оставался открытым вопрос, как построить само множество минимальных CI-функций. Минимальные CI-функции от малого числа переменных можно получить с помощью вычислительной техники. Примеры таких функций можно найти в работе [4], [5]. Для получения CI-функций от большого числа переменных в работе [3] был предложен рекурсивный метод. В работе было введено отображение AC^w и было доказано, что применение данного отображения к минимальным CI-функциям от малого числа переменных позволяет получить минимальные CI-функции от большего числа переменных. Метод прост в реализации и позволяет быстро наращивать число переменных.

Однако среди функций построенного множества могут быть совпадающие между собой функции. В данной работе сформулирован критерий равенства функций, являющихся результатом применения отображения AC^w к некоторой исходной функции. Данный критерий в дальнейшем используется при доказательстве нижней и верхней оценках мощности множеств строящихся функций. Оценки также приведены в работе.

Статья получена 01.09.2021

Е. К. Карелина работает в АО «ИнфоТеКС» (e-mail: karelinakaterina.cmc@gmail.com, Ekaterina.Karelina@infotecs.ru)

II. Основные понятия и обозначения

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 $V_n^* = V_n \backslash 0^n$, 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 $wt(u)$ вектора $u \in V_n$ называется число единиц в u. Набор $u \in V_{2^n}$ называется уравновешенным, если $wt(u) = 2^{n-1}$.

Множество всех булевых функций от n переменных $f: V_n \to \mathbb{F}_2$ 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 $supp(f) = \{ x \in V_n \mid f(x) = 1 \}$, а мощность данного множества — весом булевой функции $wt(f)$. Обозначим через $\mathcal{F}_n^w = \{f \in \mathcal{F}_n | wt(f) = w\}$.

Для функции $f \in \mathcal{F}_n$ таблицей истинности называется $(wt(f) \times n)$-матрица, строками которой являются те наборы из V_n, значение функции на которых равно 1. Считаем, что в такой матрице все строки лексикографически упорядочены сверху вниз.

Преобразованием Уолша-Адамара булевой функции $f \in \mathcal{F}_n$ называют целочисленную функцию на V_n, которая определяется равенством

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

(суммирование производится в действительной области). Для каждого $u \in V_n$ значение $W_f(u)$ называют коэффициентом Уолша-Адамара.

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:

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

Из определения следует, что все CI-функции имеют четный вес.

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

$cor(f) = \max \{c \in \mathbb{N} \mid f$ – CI-функция порядка $c\}$.

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

Справедлив следующий критерий корреляционной иммунности.

Теорема 1. [6] Булева функция $f \in \mathcal{F}_n$ корреляционно-иммунна порядка c тогда и только тогда, когда для любого вектора $u \in V_n$ такого, что $1 \leq wt(f) \leq c$, выполнено равенство $W_f(u) = 0$.

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 [7]. Обозначается $OA_\nu(m, n, 2, t)$.

Теорема 2. [7] Для любой функции $f \in \mathcal{F}_n$ выполнено неравенство $cor(f) \geq c$ тогда и только тогда, когда ее таблица истинности является ортогональным массивом $OA_\nu(wt(f), n, 2, c)$.

Для удобства дальнейшего изложения сформулируем простое следствие из Теоремы 2:

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

Очевидно, что в такой таблице все столбцы уравновешенны.

Напомним понятие минимальной CI-функции, введенное в работе [2].

Определение 1. Функция $f \in CI(n)$ называется минимальной корреляционно-иммунной функцией, если не существует корреляционно-иммунной функции $g \in CI(n)$, для которой выполняется $supp(g) \subset supp(f)$.

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

В работе [3] были введены следующие отображения и описаны их действия на функции.

$$AC^w: \mathcal{F}_n^w \times V_w \times \{1, \dots, n+1\} \mapsto \mathcal{F}_{n+1}^w,$$
$$AC_{v,i}^w(f) = AC^w(f, v, i) = g, \text{ где}$$
$$v = \left(v^{(1)}, v^{(2)}, \dots, v^{(w)}\right) \in V_w$$

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

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

где $i < n + 1$.

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

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

Действие отображения AC^w заключается в добавлении столбца длины w к таблице истинности функции.

Справедливы следующие теоремы:

Теорема 3. [3], [5] 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 $i \in \{1, \dots, n+1\}$.

Теорема 4. [3], [5] 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 $i \in \{1, \dots, n+1\}$.

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 $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2 \oplus x_2\, x_3 \oplus x_1\, x_3 \oplus x_1\, x_2\, x_3$ от 3 переменных такова:

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

III. Критерий равенства получаемых функций при использовании отображения AC^w

Применяя отображение AC^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 $a = \left(a^{(1)}, \dots, a^{(w)}\right)^T$, $b = \left(b^{(1)}, \dots, b^{(w)}\right)^T$ — 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^{w}.

Теорема 5. $f' = f''$ тогда и только тогда, когда наборы в исходной таблице истинности T_f функции f можно разбить на пары с номерами $k, m, 1 \le k \le w, 1 \le m \le w$, для которых выполняются равенства (1)-(3):

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

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

а для наборов с номерами l, где $l \ne k, m$, которые не вошли в разбиение по парам, выполняется условие (4):

а для наборов с номерами l, где $l \ne k, m$, которые не вошли в разбиение по парам, выполняется условие (4):

$$a^{(l)} = x_l^{(i)} = x_l^{(i+1)} = \dots = x_l^{(j-2)} = x_l^{(j-1)} = b^{(l)} \#(4)$$

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 $l, 1 \le l \le w$:

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

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 $k, 1 \le k \le w$, в таблице истинности T_f' равен набору с номером $m, 1 \le m \le w$, 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 будут справедливы указанные системы равенств (1)-(3), а для оставшихся наборов будут выполняться равенства (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.

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

Докажем верхнюю оценку мощности множества функций, которые получаются применением отображения AC^w к некоторой начальной функции.

Теорема 6. Пусть $f \in CI(n), wt(f) = w$.

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

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

Пусть столбец $a = \left(a^{(1)}, \dots, a^{(w)}\right)^T$ добавляется на позицию i, столбец $b = \left(b^{(1)}, \dots, b^{(w)}\right)^T$ на позицию j. Пусть полученные функции равны. Воспользуемся критерием равенства функций из Теоремы 5, получаемых при применении отображения AC^w.

Рассмотрим случай, когда в некоторых полученных таблицах истинности для всех наборов выполняется только условие (4):

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

Пусть $j = i+1, i < n+1$. Тогда

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

Из этого равенства однозначно определяются значения вектор-столбцов a, b для любого 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:

$$T_f = \binom{011}{100}.$$

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

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:

$$\binom{\mathbf{0}011}{\mathbf{1}100}, \binom{0\mathbf{0}11}{1\mathbf{1}00}, \binom{01\mathbf{0}1}{10\mathbf{1}0}, \binom{011\mathbf{0}}{100\mathbf{1}},$$

$$\binom{\mathbf{1}011}{\mathbf{0}100}, \binom{0\mathbf{1}11}{1\mathbf{0}00}, \binom{01\mathbf{1}1}{10\mathbf{0}0}, \binom{011\mathbf{1}}{100\mathbf{0}}.$$

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 6:

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

Таким образом, верхняя оценка для множества M, полученная согласно Теореме 6, справедлива, и существуют функции, для которых данная оценка достижима.

Ниже в Таблице 1, Таблице 2 и Таблице 3 приведено еще несколько примеров CI-функций с различными параметрами. Пусть A – значение верхней оценки множества M для указанных параметров. Данные значения функций и мощностей построенных множеств были получены с помощью вычислительной техники.

Таблица 1 - примеры CI-функций разного веса от 4 переменных, значения мощностей соответствующих построенных множеств M и значения верхней оценки множеств M

n	f	$wt(f)$	$\|M\|$	A
4	$0x0420$	2	5	6
4	$0x0180$	2	6	6
4	$0x2424$	4	22	26
4	$0x0690$	4	25	26
4	$0x1284$	4	26	26
4	$0x2a54$	6	86	96
4	$0x13c8$	6	90	96
4	$0x3486$	6	94	96
4	$0x1be4$	8	337	346
4	$0x6996$	8	340	346
4	$0x9696$	8	328	346

Как видно из данной таблицы, с увеличением веса исходной функции число равных функций, получаемых с помощью отображения AC^w, растет. Для меньших весов функций верхняя оценка может быть достижимой. Всего было найдено 7 CI-функций от 4 переменных веса 2 и 13 CI-функций от 4 переменных веса 4, у которых мощность соответствующего множества M достигала верхней оценки.

Таблица 2 - примеры минимальных CI-функций разного веса от 5 переменных, значения мощностей соответствующих построенных множеств M и значения верхней оценки множеств M

n	f	$wt(f)$	$\|M\|$	A
5	$0x00200400$	2	6	7
5	$0x80000001$	2	7	7
5	$0x20040420$	4	30	31
5	$0x84000012$	4	31	31
5	$0x06101088$	6	112	115
5	$0x08186001$	6	113	115
5	$0x02188410$	6	114	115
5	$0x04186002$	6	115	115
5	$0x06606009$	8	411	415
5	$0x14422881$	8	412	415

5	$0x18810660$	8	413	415
5	$0x21188442$	8	414	415
5	$0x24814812$	8	415	415

Функции из таблицы выше являются минимальными CI-функциями от 5 переменных. Всего было найдено следующее число минимальных CI-функций от 5 переменных, у которых мощность соответствующего множества M достигала верхней оценки:

- 15 минимальных CI-функций веса 2,
- 150 минимальных CI-функций веса 4,
- 372 минимальные CI-функции веса 6,
- 52 минимальные CI-функции веса 8.

Таблица 3 - примеры минимальных CI-функций разного веса от 6 переменных, значения мощностей соответствующих построенных множеств M и значения верхней оценки множеств M

n	f	$wt(f)$	$\|M\|$	A
6	$0x0000040000200000$	2	7	8
6	$0x2000000000000004$	2	8	8
6	$0x0020040000200400$	4	32	36
6	$0x0011000000008800$	4	33	36
6	$0x0000410000280000$	4	35	36
6	$0x0000400120080000$	4	36	36
6	$0x9800000000000019$	6	131	134
6	$0x3400000000000089$	6	132	134
6	$0x3080000000000409$	8	133	134
6	$0xf000000000000000f$	8	442	484
6	$0xe800000000000017$	8	466	484
6	$0xe008000000001007$	8	475	484
6	$0x9420000000000429$	8	484	484

Выше в таблице представлены некоторые минимальные CI-функции от 6 переменных. Всего было найдено следующее число минимальных CI-функций от 6 переменных, у которых мощность соответствующего множества M достигала верхней оценки:

- 31 минимальная CI-функция веса 2,
- 1649 минимальных CI-функций веса 4,
- 45255 минимальных CI-функций веса 6,
- 500375 минимальных CI-функций веса 8.

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

Теорема 7. Пусть $f \in CI(n), wt(f) = w$.

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

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

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:

$$f' = AC^w_{a,1}(f),$$
$$f'' = AC^w_{b,2}(f).$$

Обозначим T'_f и T''_f соответствующие им таблицы истинности.

Рассмотрим все возможные случаи равенства получаемых функций, используя Теорему 5.

1. Пусть для всех наборов таблиц истинности полученных функций выполнено условие (4) из Теоремы 5:
$$a^{(l)} = x_l^{(1)} = b^{(l)}, l \in [1, w].$$
Из этого равенства однозначно определяются значения вектор-столбцов a и b. Рассматриваемый случай существует всегда для любой исходной 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 (1)-(3) Теоремы 5, а для оставшихся наборов выполняется условие (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:

$$\begin{cases} a^{(k)}x_k^{(1)}x_k^{(2)}x_k^{(3)}\dots x_k^{(n)} = x_m^{(1)}b^{(m)}x_m^{(2)}x_m^{(3)}\dots x_m^{(n)} \\ a^{(m)}x_m^{(1)}x_m^{(2)}x_m^{(3)}\dots x_m^{(n)} = x_k^{(1)}b^{(k)}x_k^{(2)}x_k^{(3)}\dots x_k^{(n)} \end{cases}$$

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. Тогда по Теореме 5 верно:

$$\begin{cases} a^{(k)}x_k^{(1)}x_k^{(2)}x_k^{(3)}\dots x_k^{(n)} = x_m^{(1)}b^{(m)}x_m^{(2)}x_m^{(3)}\dots x_m^{(n)} \\ a^{(k)}x_k^{(1)}x_k^{(2)}x_k^{(3)}\dots x_k^{(n)} = x_t^{(1)}b^{(t)}x_t^{(2)}x_t^{(3)}\dots x_t^{(n)} \end{cases}$$

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

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

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

3. Пусть для части наборов выполняются условия (1)-(3) Теоремы 5. 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'':

$$\begin{cases} a^{(k_1)}x_{k_1}^{(1)}x_{k_1}^{(2)}x_{k_1}^{(3)}\dots x_{k_1}^{(n)} = x_{k_2}^{(1)}b^{(k_2)}x_{k_2}^{(2)}x_{k_2}^{(3)}\dots x_{k_2}^{(n)} \\ a^{(k_2)}x_{k_2}^{(1)}x_{k_2}^{(2)}x_{k_2}^{(3)}\dots x_{k_2}^{(n)} = x_{k_3}^{(1)}b^{(k_3)}x_{k_3}^{(2)}x_{k_3}^{(3)}\dots x_{k_3}^{(n)} \\ a^{(k_3)}x_{k_3}^{(1)}x_{k_3}^{(2)}x_{k_3}^{(3)}\dots x_{k_3}^{(n)} = x_{k_1}^{(1)}b^{(k_1)}x_{k_1}^{(2)}x_{k_1}^{(3)}\dots x_{k_1}^{(n)} \end{cases}$$

Тогда по условию (1) Теоремы 5 верны следующие равенства:

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

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 раннее при добавлении столбцов на первую позицию равно

$$1 + \sum_{i=1}^{\frac{w}{2}} \binom{w/2}{i} = 2^{w/2}.$$

Тогда верно следующее неравенство:

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

Так как рассуждения были рассмотрены лишь для случая 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:

$$T_f = \binom{0100}{1011}.$$

Построим множество функций $M' = \{f' = AC_{a,1}^2(f), f'' = AC_{b,2}^2(f), a, b,\ wt(a) = wt(b) = \frac{wt(f)}{2} = 1\}$. Множество M' является подмножеством множества M и состоит из функций, таблицы истинности которых представлены ниже:

$$\binom{\mathbf{0}0100}{\mathbf{1}1011}, \binom{0\mathbf{0}100}{1\mathbf{1}011},$$

$$\binom{\mathbf{1}0100}{\mathbf{0}1011}, \binom{0\mathbf{1}100}{1\mathbf{0}011}.$$

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 7:

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

Таким образом, данная оценка из Теоремы 7 справедлива.

Рассмотрим еще один пример. Пусть функция $f \in CI(3),\ wt(f) = 4$ задается следующей таблицей истинности:

$$T_f = \begin{pmatrix} 000 \\ 011 \\ 100 \\ 111 \end{pmatrix}.$$

Построим множество функций $M' = \{ f' = AC^4_{a,1}(f), f'' = AC^4_{b,2}(f), a, b,\ wt(a) = wt(b) = \frac{wt(f)}{2} = 2\}$. Множество M' является подмножеством множества M и состоит из функций, таблицы истинности которых представлены ниже:

$$\begin{pmatrix} \mathbf{1}000 \\ \mathbf{0}011 \\ \mathbf{0}100 \\ \mathbf{1}111 \end{pmatrix}, \begin{pmatrix} \mathbf{01}00 \\ \mathbf{00}11 \\ \mathbf{1}000 \\ \mathbf{1}111 \end{pmatrix}, \begin{pmatrix} \mathbf{0}000 \\ \mathbf{0}011 \\ \mathbf{1}100 \\ \mathbf{1}111 \end{pmatrix}, \begin{pmatrix} 0\mathbf{0}00 \\ 0\mathbf{0}11 \\ 1\mathbf{1}00 \\ 1\mathbf{1}11 \end{pmatrix}, \begin{pmatrix} \mathbf{1}000 \\ \mathbf{1}011 \\ \mathbf{0}100 \\ \mathbf{0}111 \end{pmatrix}, \begin{pmatrix} 0\mathbf{10}0 \\ 0\mathbf{11}1 \\ 1\mathbf{00}0 \\ 1\mathbf{01}1 \end{pmatrix},$$

$$\begin{pmatrix} \mathbf{0}000 \\ \mathbf{1}011 \\ \mathbf{1}100 \\ \mathbf{0}111 \end{pmatrix}, \begin{pmatrix} \mathbf{0000} \\ 0\mathbf{11}1 \\ 1\mathbf{10}0 \\ 1\mathbf{01}1 \end{pmatrix}, \begin{pmatrix} \mathbf{0}000 \\ \mathbf{1}011 \\ \mathbf{0}100 \\ \mathbf{1}111 \end{pmatrix}, \begin{pmatrix} 0\mathbf{0}00 \\ 0\mathbf{1}11 \\ 1\mathbf{0}00 \\ 1\mathbf{1}11 \end{pmatrix}, \begin{pmatrix} \mathbf{1}000 \\ \mathbf{0}011 \\ \mathbf{1}100 \\ \mathbf{0}111 \end{pmatrix}, \begin{pmatrix} 0\mathbf{10}0 \\ 0\mathbf{0}11 \\ 1\mathbf{1}00 \\ 1\mathbf{0}11 \end{pmatrix}.$$

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 7:

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

Таким образом, данная оценка из Теоремы 7 справедлива.

VI. Заключение

В настоящей работе доказан критерий равенства функций, которые получаются после применения отображения AC^w к некоторой исходной функции f. Данный критерий используется при доказательстве верхней и нижней оценки мощности множества функций, которые можно получить, используя отображение AC^w.

Библиография

[1] Ю. В. Тарannиков, “О корреляционно-иммунных и устойчивых булевых функциях”, *Математические вопросы кибернетики*, 11 (2002), 91-148

[2] Е. К. Алексеев, “О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций”, *Дискретная математика*, 22:3 (2010), 110-126, http://mi.mathnet.ru/dm1111

[3] Alekseev E.K., Karelina E.K., Logachev O.A., “On construction of correlation-immune functions via minimal functions”, *Математические вопросы криптографии*, 9:2, (2018), 7–21, http://mi.mathnet.ru/mvk251

[4] Е. К. Алексеев, Е. К. Карелина, “Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных”, *Дискретная математика*, 27:1 (2015), 22–33, http://mi.mathnet.ru/dm1312

[5] Е. К. Карелина, “Об одном методе синтеза корреляционно-иммунных булевых функций”, *Дискретная математика*, 30:4 (2018), 12-28, http://mi.mathnet.ru/dm1524

[6] О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Ященко *Булевы функции в теории кодирования и криптологии*, Ленанд, 2015, 576 pp

[7] Ю. В. Тарannиков, *Комбинаторные свойства дискретных структур и приложения к криптологии*, МЦНМО, 2011, 152 pp

Some cardinality estimates for the set of correlation-immune Boolean functions obtained by the mapping AC^w

E. K. Karelina

***Abstract* — The mapping AC^w was introduced in one of the works devoted to the study of correlation-immune functions. This mapping allows to quickly increase the number of function's variables. It is the base of recursive method of synthesis correlation-immune Boolean functions. However, applying a mapping to the function with all possible parameters allows constructing functions, which is equal to each other. In this paper, there is a criterion of functions equality, which can be produced by AC^w mapping. Also, lower and upper bounds for the set of correlation-immune functions obtained using this mapping are proved. In the proof of these estimates, the function equality criterion is used. The paper presents examples of correlation-immune functions of various weights of a small number of variables and the values of the cardinalities of the corresponding sets, which are obtained by applying the mapping AC^w to the given correlation-immune functions. These results are obtained using computer and they confirm the proved upper and lower bounds for the considered sets of functions.**

***Keywords* — correlation-immune functions, construction of correlation-immune functions, cardinality, upper bound, lower bound.**

REFERENCES

[1] Y. V. Tarannikov, "Correlation-immune and resilient Boolean functions", *Mathematical Problems of Cybernetics*, 11 (2002), 91-148

[2] E. K. Alekseev, "Some algebraic and combinatorial properties of correlation-immune Boolean functions", *Discrete Math.*, 22:3 (2010), 110-126, http://mi.mathnet.ru/dm1111

[3] Alekseev E.K., Karelina E.K., Logachev O.A., "On construction of correlation-immune functions via minimal functions", *Mathematical Problems of Cryptography*, 9:2, (2018), 7–21, http://mi.mathnet.ru/mvk251

[4] E. K. Alekseev, E. K. Karelina, "Classification of correlation-immune and minimal correlation-immune Boolean functions of 4 and 5 variables", *Discrete Math.*, 27:1 (2015), 22–33, http://mi.mathnet.ru/dm1312

[5] E. K. Karelina, "On a method of synthesis of correlation-immune Boolean functions", *Discrete Math.*, 30:4 (2018), 12–28, http://mi.mathnet.ru/dm1524

[6] O. A. Logachev, A. A. Salnikov, S. V. Smyshlyaev, V. V. Yashchenko, *Boolean functions in coding theory and cryptology*, URSS. ISBN 978-5-9710-0961-0, 576 c., 2015

[7] Y. V. Tarannikov, *Combinatorial properties of discrete structures and applications to cryptology*, ISBN 978-5-94057-812-3, 2011, 152 pp