



Math-Net.Ru

Общероссийский математический портал

П. В. Ролдугин, А. В. Тарасов, Функции без коротких имплицент. Часть I: нижние оценки весов, *Дискрет. матем.*, 2015, том 27, выпуск 2, 94–105

DOI: 10.4213/dm1327

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.97.9.173

20 марта 2025 г., 21:46:51



Функции без коротких имплициент. Часть I: нижние оценки весов

© 2015 г. П. В. Ролдугин*, А. В. Тарасов**

В статье рассматриваются булевы функции от n переменных, не имеющие имплициент от k , $1 \leq k < n$, переменных. Получены оценки минимально возможного веса $w(n, k)$ таких функций. Показано, что $w(n, 1) = 2$, $n = 2, 3, \dots$, и $w(n, 2) \sim \log_2 n$ при $n \rightarrow \infty$, а для $k > 2$ существует такое n_0 , что $w(n, k) > 2^{k-2} \cdot \log_2 n$ при всех $n > n_0$.

Ключевые слова: булевы функции, имплициенты, комбинаторно полные матрицы.

Введение и обзор результатов. Введем ряд обозначений и определений:

- V_n – множество двоичных векторов длины n ;
- E_f – множество выполняющих векторов булевой функции $f(x_1, \dots, x_n)$ от n переменных, то есть $E_f = \{(\alpha_1, \dots, \alpha_n) \in V_n : f(\alpha_1, \dots, \alpha_n) = 1\}$;
- $\|f\| = |E_f|$ – вес функции f ;
- $\|\alpha\|$ – вес вектора $\alpha \in V_n$;
- $f \equiv g$ – равенство булевых функций f и g ;
- $\bar{f} = f \oplus 1$ – инверсия функции f ;
- для булевой переменной x и $\alpha \in \{0, 1\}$ обозначим

$$x^\alpha = \begin{cases} \bar{x}, & \alpha = 0; \\ x, & \alpha = 1. \end{cases}$$

Имплицентой булевой функции $f(x_1, \dots, x_n)$ называется такая не равная константе булева функция g , что $f \cdot g \equiv f$, что эквивалентно включению $E_f \subseteq E_g$ (см. [1]). В печати встречаются и другие определения, схожие с понятием имплициенты. Например, в [2]-[5] используется понятие аннигилятора булевой функции f : *аннигилятором* функции f называется такая функция h , что $f \cdot h \equiv 0$. Очевидно, что h – аннигилятор функции f тогда и только тогда, когда функция $\bar{h} = h \oplus 1$ – имплициента функции f . Иногда (см. [7]) имплициенту булевой функции f называют верхним аналогом функции f (см. [4]). В широко известной проблематике минимизации ДНФ (см. [9]) используется определение импликанты булевой функции (функция g называется *импликантой* функции f , когда $f \vee g = g$), двойственное понятию имплициенты (см., например, [3]). Существует известная очевидная связь

*Место работы: Московский государственный технический университет радиотехники, электроники и автоматики, e-mail: PavRoldugin@rambler.ru

**Место работы: Московский государственный технический университет радиотехники, электроники и автоматики, e-mail: alextar1@yandex.ru

между понятиями имплицента и импликанты булевой функции f : g – имплицента функции f тогда и только тогда, когда \bar{g} – импликанта функции \bar{f} . Соответственно, можно с очевидными изменениями переформулировать основные результаты статьи в указанных выше терминах.

В настоящей статье изучаются оценки минимально возможного значения веса булевой функции, не имеющей имплицентов, зависящих от не более чем k переменных. Похожие вопросы затронуты, например, в работе [5], в которой приводятся некоторые условия существования аннигиляторов с ограничениями на количество существенных переменных. Например, следствие 3 из настоящей работы можно достаточно просто вывести и из результатов [5]. С другой стороны, при изучении аннигиляторов булевых функций основное внимание уделяется исследованию алгебраической иммунности функций, которая определяется как минимально возможная степень аннигилятора функции f или $f \oplus 1$. Малое число переменных аннигилятора влечет за собой и ограничение на его степень. Однако, отсутствие у функции f аннигиляторов, зависящих не более чем от k переменных, вообще говоря, не накладывает ограничений на значение алгебраической иммунности функции f .

Длиной булевой функции назовем число ее существенных переменных; длину функции-константы (0 или 1) будем считать равной 0.

Зафиксируем натуральные числа n и k , $n > k \geq 1$. Рассмотрим класс $G_n^{(k)}$ булевых функций от n переменных, не имеющих имплицентов длины k или меньше. Отметим, что при $n = k$ у отличной от константы функции от n переменных всегда есть имплицента длины n – это она сама. Поэтому данный случай исключен из рассмотрения. При $n > k \geq 1$ класс $G_n^{(k)}$ не пуст. Например, в этом классе лежит любая функция от n переменных, имеющая вес $2^n - 1$. Действительно, если у функции f $E_f = V_n \setminus \{(\alpha_1, \dots, \alpha_n)\}$, то $f(x_1, \dots, x_n) = x_1^{\alpha_1 \oplus 1} \vee \dots \vee x_n^{\alpha_n \oplus 1}$. Если g – имплицента функции f , то по определению $E_f \subseteq E_g$ и $E_g \neq V_n$, следовательно, $E_f = E_g$, то есть $f \equiv g$. У функции f все переменные, очевидно, существенные, поэтому длина функции g равна n и не равняется k при $k < n$. Значит, у функции f нет имплицентов длины k . Таким образом, класс $G_n^{(k)}$ не пуст при $k < n$.

Ввиду сказанного корректно ввести обозначение $w(n, k)$ для минимального веса функции из класса $G_n^{(k)}$.

Если булева функция от n переменных имеет вес 0, то ее имплицентами являются все не равные константе булевы функции от n переменных. Следовательно, при любых n и k , $n > k$, функция, тождественно равная нулю, не лежит в классе $G_n^{(k)}$, и поэтому $w(n, k) > 0$.

Целью настоящей статьи является нахождение нижних оценок величины $w(n, k)$ для различных n и k , $n > k$. При $k = 1$ задача решается очень просто.

Утверждение 1. При любом натуральном $n \geq 2$ верно равенство $w(n, 1) = 2$.

Доказательство. Функций веса 1 без имплицентов длины 1 не существует, поскольку, если функция f принимает значение 1 на единственном наборе $(\alpha_1, \dots, \alpha_n) \in V_n$, то $f(x_1, \dots, x_n) = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ и тогда любая функция $g = x_i^{\alpha_i}$ является имплицентовой функции f . Следовательно, $w(n, 1) \geq 1$. Кроме того, можно прямо указать функцию веса 2 от n переменных, не имеющую имплицентов длины 1 – это функция $f(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n \vee \bar{x}_1 \cdot \dots \cdot \bar{x}_n$. Действительно, для любых $i \in \overline{1, n}$ и $\alpha \in \{0, 1\}$ верно: $x_i^\alpha \cdot f = x_1^\alpha \cdot \dots \cdot x_n^\alpha \neq x_1 \cdot \dots \cdot x_n \vee \bar{x}_1 \cdot \dots \cdot \bar{x}_n = f$. Поэтому $w(n, 1) = 2$.

Кроме рассмотренного случая $k = 1$ получить асимптотически точное значение величины $w(n, k)$ удалось только для случая $k = 2$: ниже показано, что

$w(n, k) \sim \log_2 n$ при $n \rightarrow \infty$. Для случая $k \geq 3$ в настоящей статье доказано существование такого n_0 , что $w(n, k) > 2^{k-2} \cdot \log_2 n$ для всех $n \geq n_0$. Кроме того, показано, что $\min_{n>k} w(n, k) = 2^k$ и, если $w(n, k) = 2^k$, то $n = k + 1$.

1. Связь функций без коротких имплицентов с комбинаторно полными матрицами. Имплицента называется *элементарной*, если существует ее запись в виде элементарной дизъюнкции. Следующее простое утверждение позволяет свести изучение функций, не имеющих коротких имплицентов, к изучению функций, не имеющих коротких элементарных имплицентов.

Утверждение 2. Булева функция f , отличная от константы, имеет имплиценту длины k тогда и только тогда, когда функция f имеет элементарную имплиценту длины k .

Доказательство. Пусть $g(x_{i_1}, \dots, x_{i_k})$ – имплицента функции $f(x_1, \dots, x_n)$. Представим функцию g в виде совершенной КНФ:

$$g = \prod_{(a_1, \dots, a_k) \in V_n \setminus E_g} (x_{i_1}^{a_1 \oplus 1} \vee \dots \vee x_{i_k}^{a_k \oplus 1}).$$

Рассмотрим любую из элементарных дизъюнкции этой совершенной КНФ вида $K = x_{i_1}^{a_1 \oplus 1} \vee \dots \vee x_{i_k}^{a_k \oplus 1}$, $(a_1, \dots, a_k) \in V_n \setminus E_g$. Она имеет k существенных переменных. Далее имеем:

$$f \cdot K \equiv (f \cdot g) \cdot K \equiv f \cdot (g \cdot K) \equiv f \cdot g \equiv f,$$

то есть K является имплицентой функции f .

В обратную сторону утверждение очевидно.

Отсутствие у булевой функции элементарных имплицентов имеет наглядный комбинаторный смысл. Введем следующее определение.

Определение 1. Пусть k , $1 \leq k < n$, – натуральное число. Назовем $(0, 1)$ -матрицу A размера $m \times n$ *комбинаторно полной порядка k* , если в любой ее подматрице размера $m \times k$ для любого булевого вектора \vec{v} длины k найдется строка, совпадающая с \vec{v} .

Иначе говоря, для любых k столбцов матрицы A образованная ими подматрица должна содержать каждую из 2^k возможных строк (не обязательно только по одному разу).

Укажем несколько простых свойств комбинаторно полных матриц. Очевидно, что $m \geq 2^k \geq 2$. Ясно, что матрица, комбинаторно полная порядка k , $k \geq 2$, является комбинаторно полной порядка s при всех $s < k$. Очевидно также, что инвертирование любого столбца комбинаторно полной матрицы (то есть инвертирование всех его элементов) приводит также к комбинаторно полной матрице того же порядка. В частности, инвертирование всей матрицы также дает комбинаторно полную матрицу а добавление любого числа произвольных строк к комбинаторно полной матрице также дает комбинаторно полную матрицу того же порядка.

Приведем пример. Зафиксируем значения n и k , $n \geq k$. Рассмотрим матрицу A , строками которой являются все возможные векторы длины n веса k . Матрица имеет $\binom{n}{k}$ строк. Выберем в матрице A произвольные k столбцов. В каждой строке матрицы A в координатах, соответствующих $n - k$ не выбранным столбцам, можно разместить не более $(n - k)$ единиц; остальные единицы окажутся в выбранных k

столбцах. Поэтому полученная подматрица будет содержать все возможные строки длины k , имеющие вес не менее $t = \max\{0, 2k - n\}$. Тогда при $n \geq 2k$ указанная подматрица будет содержать все строки длины k , откуда следует, что сама матрица A является комбинаторно полной порядка k .

В данном примере число m строк в матрице A при небольших фиксированных значениях k и растущем значении n ведет себя как $O(n^k)$. Однако можно построить комбинаторно полные матрицы и с существенно меньшим числом строк. Собственно нахождение минимального значения числа строк комбинаторно полной матрицы и составляет основную цель данной работы. Это обусловлено простой связью, существующей между комбинаторно полными матрицами и булевыми функциями, не имеющими элементарных имплицинт. Матрицу, строки которой являются выполняющими векторами булевой функции f от n переменных, обозначим через \tilde{E}_f , то есть

$$\tilde{E}_f = \begin{pmatrix} (\alpha_1^{(1)}, \dots, \alpha_n^{(1)}) \\ \dots \\ (\alpha_1^{(\|f\|)}, \dots, \alpha_n^{(\|f\|)}) \end{pmatrix},$$

где $(\alpha_1^{(i)}, \dots, \alpha_n^{(i)}) \in E_f, i = \overline{1, \|f\|}$.

Следующее утверждение является естественным обобщением аналогичного утверждения для случая $k = 2$, доказанного в [8]. Вместе с тем, легко показать, что оно эквивалентно теореме 1.1 работы [5].

Утверждение 3. Булева функция f , отличная от константы, имеет элементарную имплицинту длины k тогда и только тогда, когда матрица \tilde{E}_f не является комбинаторно полной порядка k .

Доказательство. Рассмотрим элементарную дизъюнкцию длины $k: g = x_{i_1}^{a_1} \vee \dots \vee x_{i_k}^{a_k}$. Эта дизъюнкция является имплицинтной функции f тогда и только тогда, когда $f \cdot g \equiv f \cdot (x_{i_1}^{a_1} \vee \dots \vee x_{i_k}^{a_k}) \equiv f$. Последнее равенство эквивалентно тому, что на всех таких векторах $(\alpha_1, \dots, \alpha_n)$, что $\alpha_{i_j} = a_j \oplus 1, j = \overline{1, k}$, должно выполняться равенство $f(x_1, \dots, x_n) = 0$. Иначе говоря, среди выполняющих векторов функции f нет таких, в которых на местах i_1, \dots, i_k стоят значения $a_1 \oplus 1, \dots, a_k \oplus 1$ соответственно. По определению, это происходит тогда и только тогда, когда в столбцах i_1, \dots, i_k матрицы \tilde{E}_f не содержится строк вида $(a_1 \oplus 1, \dots, a_k \oplus 1)$, то есть матрица \tilde{E}_f не является комбинаторно полной порядка k .

Пусть $m_{\min}^{(k)}(n)$ – минимальное число строк в комбинаторно полной матрице порядка k с n столбцами, $n > k$.

Следствие 1. При любых натуральных n и $k, n > k \geq 1$, верно равенство

$$w(n, k) = m_{\min}^{(k)}(n).$$

Доказательство. Из доказанного утверждения 3 следует, что если булева функция f от n переменных не имеет имплицинт длины k и ее вес равен $w(n, k)$, то матрица \tilde{E}_f с $w(n, k)$ строками и n столбцами является комбинаторно полной порядка k . Следовательно $w(n, k) \geq m_{\min}^{(k)}(n)$. С другой стороны, рассмотрим комбинаторно полную матрицу порядка k , имеющую $m_{\min}^{(k)}(n)$ строк и n столбцов. В этой матрице отсутствуют одинаковые строки – в противном случае, удалив повторы,

придем к комбинаторно полной матрице порядка k , имеющей n столбцов и меньше $m_{\min}^{(k)}(n)$ строк, что невозможно по определению величины $m_{\min}^{(k)}(n)$. В частности, отсутствие одинаковых строк означает, что $m_{\min}^{(k)}(n) \leq 2^n$. Но в этом случае матрицу можно рассмотреть как матрицу \tilde{E}_f для функции f , задаваемой следующим способом: $E_f = \{\vec{A}_1, \vec{A}_2, \dots, \vec{A}_{m_{\min}^{(k)}(n)}\}$, где \vec{A}_i – строки матрицы A . Функция f от n переменных веса $m_{\min}^{(k)}(n)$ не имеет имплицент в силу утверждения 3, и поэтому получаем обратное неравенство $w(n, k) \leq m_{\min}^{(k)}(n)$, что и доказывает данное следствие.

Поскольку у комбинаторно полной матрицы порядка k не может быть меньше 2^k строк, то получаем первую оценку величины $w(n, k)$.

Следствие 2. При любых натуральных n и k , $n > k \geq 1$, верно неравенство

$$w(n, k) \geq 2^k.$$

Двойственной задачей к вычислению $m_{\min}^{(k)}(n)$ является нахождение для фиксированного числа строк m максимального значения $n_{\max}^{(k)}(m)$ числа столбцов, при котором существует комбинаторно полная матрица размера $m \times n_{\max}^{(k)}(m)$ порядка k . В терминах булевых функций такая задача сводится к поиску при фиксированных m и k функции веса m от наибольшего числа переменных, не имеющей имплицент длины k .

Отметим, что значение $m_{\min}^{(k)}(n)$ определено при всех $k \geq 1$; значение же величины $n_{\max}^{(k)}(m)$ определяется только при $k > 1$, поскольку при $k = 1$ в качестве комбинаторно полной матрицы порядка 1 можно взять матрицу $\begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \end{pmatrix}$, имеющую всего две строки, но произвольное число столбцов. Поэтому далее будем рассматривать только случай $k > 1$.

При фиксированном $k > 1$ значение $n_{\max}^{(k)}(m)$ определено при всех $m \geq 2^k$. Функция $n_{\max}^{(k)}(m)$ является неубывающей, то есть $n_{\max}^{(k)}(m) \leq n_{\max}^{(k)}(m+1)$, поскольку, как отмечалось выше, в комбинаторно полную матрицу можно добавлять любые строки. Однако не доказано, что при любом фиксированном k функция $n_{\max}^{(k)}(m)$ является строго возрастающей (этот факт доказан только при $k = 2$ – см. [8]). Аналогично, поскольку из комбинаторно полной матрицы порядка k с более чем k столбцами можно удалить любой столбец и матрица останется комбинаторно полной, функция $m_{\min}^{(k)}(n)$, $n > k > 1$, является неубывающей.

В некоторых случаях функцию $n_{\max}^{(k)}(m)$ выписать в явном виде проще, чем функцию $m_{\min}^{(k)}(n)$ (примером может служить случай $k = 2$, разобранный, как уже указывалось, в [8]). Зададимся вопросом: каким образом от функции $n_{\max}^{(k)}(m)$ можно перейти к функции $m_{\min}^{(k)}(n)$ и, пользуясь следствием 1 утверждения 3, получить значение $w(n, k)$?

Связь между значениями $m_{\min}^{(k)}(n)$ и $n_{\max}^{(k)}(m)$ устанавливается в следующем утверждении.

Утверждение 4. Пусть n_0, k – натуральные числа, причем $n_0 > k > 1$. Возможен один из двух случаев:

1) при некотором натуральном значении $m_0 \geq 2^k + 1$ верны неравенства

$$n_{\max}^{(k)}(m_0 - 1) < n_0 \leq n_{\max}^{(k)}(m_0),$$

и тогда $m_{\min}^{(k)}(n_0) = m_0$, $w(n_0, k) = m_0$;

2) верно неравенство

$$n_0 \leq n_{\max}^{(k)}(2^k),$$

тогда $m_{\min}^{(k)}(n_0) = 2^k$, $w(n_0, k) = 2^k$.

Доказательство. Поскольку, как показано выше, область значений функции $n_{\max}^{(k)}(m)$, $m \geq 4$, $k > 1$, ограничена снизу значением $n_{\max}^{(k)}(2^k)$ и не ограничена сверху, то для значения n_0 действительно возможен только один из двух указанных в формулировке случаев. Рассмотрим первый случай: пусть существует такое $m_0 \geq 2^k + 1$, что $n_{\max}^{(k)}(m_0 - 1) < n_0 \leq n_{\max}^{(k)}(m_0)$. Неравенство $n_0 \leq n_{\max}^{(k)}(m_0)$ означает, что существует комбинаторно полная матрица порядка k и размера $m_0 \times n_0$. Отсюда следует, что $m_{\min}^{(k)}(n_0) \leq m_0$. Докажем, что $m_{\min}^{(k)}(n_0) = m_0$. От противного: пусть $m_{\min}^{(k)}(n_0) = m'_0$ и $m'_0 < m_0$. Тогда существует комбинаторно полная матрица размера $m'_0 \times n_0$. Добавляя в эту матрицу $m_0 - m'_0 - 1$ произвольных строк, получаем комбинаторно полную матрицу порядка k размера $(m_0 - 1) \times n_0$. То есть $n_0 \leq n_{\max}^{(k)}(m_0 - 1)$, что противоречит условию. Второй случай очевиден.

Более простой вид имеет утверждение, которое позволяет рассматривать верхние оценки величины $n_{\max}^{(k)}(m)$ как нижние оценки функции $m_{\min}^{(k)}(n)$, и наоборот.

Утверждение 5. Пусть n_0, m_0, k — натуральные числа, причем $n_0 > k > 1$, $m_0 \geq 2^k$. Неравенство $n_{\max}^{(k)}(m_0) < n_0$ верно тогда и только тогда, когда верно неравенство $m_{\min}^{(k)}(n_0) > m_0$.

Доказательство. Оба неравенства, очевидно, эквивалентны тому, что не существует комбинаторно полной матрицы размера $m_0 \times n_0$ порядка k .

Далее в статье приводятся нижние оценки значений $w(n, k)$: оценивается сверху значение функции $n_{\max}^{(k)}(m)$, далее на основе утверждений 4 или 5, выводятся нижние оценки величины $m_{\min}^{(k)}(n)$, которые, в силу следствия 1 утверждения 3, являются нижними оценками для $w(n, k)$.

2. Верхние оценки величины $n_{\max}^{(k)}(m)$. Начнем с рассмотрения комбинаторно полных матриц порядка k с минимально возможным значением числа строк $m = 2^k$.

Утверждение 6. Для любого $k > 1$ верно равенство $n_{\max}^{(k)}(2^k) = k + 1$.

Доказательство. Рассмотрим произвольную комбинаторно полную порядка k матрицу A размера $2^k \times (k + 1)$. Её первые k столбцов содержат 2^k различных строк. Следовательно, совокупность всех строк матрицы есть совокупность битовых строк длины $k + 1$ вида $\{(\alpha_1, \dots, \alpha_k, \beta_{(\alpha_1, \dots, \alpha_k)}) : (\alpha_1, \dots, \alpha_k) \in V_k\}$.

Докажем, что матрица A является комбинаторно полной порядка k тогда и только тогда, когда для любого $i \in \overline{1, k}$ верно равенство

$$\beta_{(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_k)} \oplus \beta_{(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_k)} = 1. \quad (1)$$

Действительно, первые k столбцов в матрице содержат все возможные 2^k строк. Выберем любые другие k столбцов матрицы A — это эквивалентно тому, чтобы выбрать $i \in \overline{1, k}$ и рассмотреть столбцы с номерами $1, 2, \dots, i - 1, i + 1, \dots, k, k + 1$. В выбранной подматрице A_i рассмотрим $k - 1$ первых столбцов. Обозначим эту подматрицу (размера $2^k \times (k - 1)$) через A'_i . Матрица A'_i содержит в качестве строк

все возможные векторы длины $k - 1$, причем каждый из векторов – ровно по два раза. Соответственно, для того, чтобы матрица A_i содержала в качестве строк все векторы длины k , необходимо и достаточно, чтобы одинаковые строки матрицы A_i продолжались в матрице A_i различными элементами, что и означает равенство (1).

Теперь рассмотрим граф булевого куба G_k , множеством вершин которого является множество V_k двоичных векторов длины k , и две вершины смежны, если соответствующие им векторы – соседние, то есть отличаются ровно в одной компоненте. Известно, что граф G_k связан и двудолен: одна из долей образована вершинами $(\alpha_1, \dots, \alpha_k)$ четного веса, другая – нечетного веса.

Заметим, что наличие последнего столбца в матрице A можно трактовать как приписывание каждой вершине $(\alpha_1, \dots, \alpha_k)$ графа G_k метки $\beta_{(\alpha_1, \dots, \alpha_k)}$, равной 0 или 1. Равенство (1) означает, что смежные вершины имеют различные метки – иначе говоря, равенство (1) эквивалентно тому, что на всех вершинах $(\alpha_1, \dots, \alpha_k)$ с четным количеством единиц (на первой доле графа G_k) метка $\beta_{(\alpha_1, \dots, \alpha_k)}$ равна некоторому значению $\nu \in \{0, 1\}$, а на всех векторах $(\alpha_1, \dots, \alpha_k)$ с нечетным количеством единиц (на второй доле графа G_k) метка $\beta_{(\alpha_1, \dots, \alpha_k)}$ равна $\bar{\nu}$. Запишем это в виде следующего равенства: для любого вектора $(\alpha_1, \dots, \alpha_k) \in V_k$

$$\alpha_1 \oplus \dots \oplus \alpha_k \oplus \nu = \beta_{(\alpha_1, \dots, \alpha_k)}. \quad (2)$$

То есть весь последний столбец матрицы A определяется значением бита ν . Значит, возможных значений этого столбца всего два и один из этих столбцов является инверсией другого.

Предположим, что существует комбинаторно полная матрица B порядка k размера $2^k \times (k + 2)$. Рассматривая подматрицы $(B_1^\downarrow, \dots, B_k^\downarrow, B_{k+1}^\downarrow)$ и $(B_1^\downarrow, \dots, B_k^\downarrow, B_{k+2}^\downarrow)$, получаем две комбинаторно полные порядка k матрицы размера $2^k \times (k + 1)$. Далее по вышесказанному получаем, что столбцы B_{k+1}^\downarrow и B_{k+2}^\downarrow либо совпадают, либо один является отрицанием другого. В обоих случаях получаем противоречие, поскольку матрица B даже не комбинаторно полная порядка 2, если рассмотреть два последних столбца.

Следовательно, наибольшее число столбцов в комбинаторно полной матрице порядка k равно $k + 1$, откуда $n_{\max}^{(2)}(k) = k + 1$.

Обратимся к исследованию случая $m > 2^k$. В работе [8] для случая $k = 2$ найдено точное значение этой функции:

$$n_{\max}^{(2)}(m) = \begin{cases} \frac{1}{2} \cdot \binom{2r}{r}, & m = 2r, \\ \binom{2r}{r-1}, & m = 2r + 1, \end{cases} \quad m \geq 4.$$

Далее рассмотрим случай $k \geq 3$.

Утверждение 7. Пусть $k \geq 3$ и $m \geq 2^k$. Тогда

$$n_{\max}^{(k)}(m) \leq n_{\max}^{(k-1)}\left(\left\lceil \frac{m}{2} \right\rceil\right) + 1.$$

Доказательство. Пусть A – комбинаторно полная матрица порядка k размера $m \times n$, $n = n_{\max}^{(k)}(m)$. В силу того, что свойство «быть комбинаторно полной матрицей» инвариантно относительно перестановки строк и столбцов матрицы, будем

В итоге при $r = k - 2$ имеем:

$$n_{\max}^{(k)}(m) \leq n_{\max}^{(2)}\left(\left[\frac{m}{2^{k-2}}\right]\right) + k - 2.$$

Воспользуемся асимптотической формулой для функции $n_{\max}^{(2)}(m)$ с целью получения асимптотической оценки функции $n_{\max}^{(k)}(m)$.

Утверждение 9. Пусть $k \geq 3$ – фиксированное число. Тогда при $m \rightarrow \infty$

$$n_{\max}^{(k)}(m) \leq 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}} \cdot (1 + o(1)).$$

Доказательство. Из следствия 4 теоремы 1 статьи [8] следует, что при $m \rightarrow \infty$ выполняется равенство

$$n_{\max}^{(2)}(m) = \frac{2^m}{\sqrt{2\pi m}} (1 + \phi(m)), \quad \lim_{m \rightarrow \infty} \phi(m) = 0. \quad (3)$$

Подставляя это соотношение в оценку из утверждения 8, получаем

$$n_{\max}^{(k)}(m) \leq \frac{2^{\left[\frac{m}{2^{k-2}}\right]}}{\sqrt{2\pi \left[\frac{m}{2^{k-2}}\right]}} \cdot (1 + \phi(m)) + k - 2.$$

Учитывая, что при $k > 0$ верны неравенства $\frac{m}{2^{k-2}} - 1 \leq \left[\frac{m}{2^{k-2}}\right] \leq \frac{m}{2^{k-2}}$, имеем:

$$\begin{aligned} n_{\max}^{(k)}(m) &\leq \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{2\pi \left(\frac{m}{2^{k-2}} - 1\right)}} \cdot (1 + \phi(m)) + k - 2 \leq \\ &\leq \sqrt{\frac{2^{k-3}}{\pi}} \cdot \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{m}} \cdot \left(\left(1 - \frac{2^{k-2}}{m}\right)^{-1/2} \cdot (1 + \phi(m)) + (k - 2) \cdot \sqrt{\frac{\pi}{2^{k-3}}} \cdot \frac{\sqrt{m}}{2^{\frac{m}{2^{k-2}}}} \right). \quad (4) \end{aligned}$$

Поскольку $k \geq 3$, то $2^{k-2}\sqrt{2} > 1$, следовательно, $\frac{\sqrt{m}}{\left(\frac{2^{k-2}\sqrt{2}}{m}\right)^m} \xrightarrow{m \rightarrow \infty} 0$. Кроме того, $\frac{2^{k-2}}{m} \xrightarrow{m \rightarrow \infty} 0$. Поэтому правая часть неравенства (4) равна $2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}} (1 + \phi(m)) = 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}} (1 + o(1))$ при $m \rightarrow \infty$.

3. Нижние оценки величины $m_{\min}^{(k)}(n)$. В этом параграфе приведены нижние оценки величины $m_{\min}^{(k)}(n)$, вытекающие из верхних оценок $n_{\max}^{(k)}(m)$, полученных в предыдущем пункте.

Начнем с равенства $n_{\max}^{(k)}(2^k) = k + 1$, $k > 1$, доказанного в утверждении 6. Этот результат можно переформулировать следующим образом, уточняющим следствие 2 утверждения 3: если $w(n, k) = 2^k$, то $n = k + 1$. То есть, среди всех булевых функций, не имеющих имплицент длины k или меньше, функции с наименьшим весом (равным 2^k) зависят не более чем от $k + 1$ переменной, и эта оценка достижима. Достигается эта оценка на тех функциях f , для которых, согласно равенству (2), для любого вектора $(\alpha_1, \dots, \alpha_{k+1}) \in E_f$ справедливо равенство $\alpha_1 \oplus \dots \oplus \alpha_k \oplus \nu = \alpha_{k+1}$ при некотором фиксированном $\nu \in \{0, 1\}$. Очевидно, что таких функции всего две: $f(x_1, \dots, x_{k+1}) = x_1 \oplus \dots \oplus x_{k+1}$ и $f(x_1, \dots, x_{k+1}) = x_1 \oplus \dots \oplus x_{k+1} \oplus 1$. Таким образом, доказано следующее утверждение.

Утверждение 10. Среди всех булевых функций, не имеющих имплицента от $k > 1$ переменных, минимальное значение веса функции равно 2^k и достигается это значение на двух функциях: $f(x_1, \dots, x_{k+1}) = x_1 \oplus \dots \oplus x_{k+1}$, $f(x_1, \dots, x_{k+1}) = x_1 \oplus \dots \oplus x_{k+1} \oplus 1$.

Важным частным случаем утверждения 10 является случай $k = n - 1$. Покажем, что если функция имеет имплиценту от k переменных, то она имеет имплиценты и от k' переменных для всех значений k' , $n > k' > k$. Действительно, если g — имплицента длины k функции $f(x_1, \dots, x_n)$ и x_i — несущественная переменная функции g , то функция $x_i \vee g$ также имплицента функции f , причем длины $k + 1$:

$$f \cdot (x_i \vee g) = \begin{cases} f, x_i = 1 \\ f \cdot g = f, x_i = 0 \end{cases} .$$

Значит, выражение "у функции от n переменных нет имплицента от $n - 1$ переменных" эквивалентно выражению "у функции от n переменных нет имплицента от меньшего числа переменных". Таким образом, из утверждения 10 при $k = n - 1$ можно сделать следующий вывод.

Следствие 3. Любая равновероятная булева функция от n переменных, отличная от функций $f(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$ и $f(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n \oplus 1$, имеет имплиценту от меньшего числа переменных.

Отметим, что данное следствие также можно легко получить из результатов работы [5].

Далее получим асимптотически точное значение величины $m_{\min}^{(2)}(n)$.

Утверждение 11. При $n \rightarrow \infty$ верно соотношение

$$m_{\min}^{(2)}(n) \sim \log_2 n.$$

Доказательство. Сначала докажем, что $m_{\min}^{(2)}(n) \rightarrow \infty$ при $n \rightarrow \infty$. Для любого $m_0 \geq 2^k > 4$ обозначим $n_0 = n_{\max}^{(2)}(m_0)$. Тогда для любого $n > n_0$ верно неравенство: $n_{\max}^{(2)}(m_0) < n$. По утверждению 5, последнее неравенство эквивалентно неравенству $m_{\min}^{(2)}(n) > m_0$. То есть, для любого $m_0 > 4$ найдется такое n_0 , что для всех $n > n_0$ выполнено $m_{\min}^{(2)}(n) > m_0$. Это и означает, что $m_{\min}^{(2)}(n) \rightarrow \infty$ при $n \rightarrow \infty$.

Поскольку функция $n_{\max}^{(2)}(m)$ является неубывающей, то из утверждения 6 следует, что минимальное значение функции $n_{\max}^{(2)}(m)$ равно 3. Подставляя это значение в утверждение 4, получаем следующее: для любого $n \geq 4$ найдется такое значение $m \geq 5$, что значение функции $m_{\min}^{(2)}(n)$ удовлетворяет неравенствам

$$n_{\max}^{(2)}(m_{\min}^{(2)}(n) - 1) < n \leq n_{\max}^{(2)}(m_{\min}^{(2)}(n)). \tag{5}$$

Поскольку $m_{\min}^{(2)}(n) \rightarrow \infty$ при $n \rightarrow \infty$, то, используя соотношение (3) из доказательства утверждения 9 и неравенства (5), получаем, что

$$\begin{aligned} \frac{2^{m_{\min}^{(2)}(n)-1}}{\sqrt{2\pi \cdot (m_{\min}^{(2)}(n) - 1)}} \left(1 + \phi(m_{\min}^{(2)}(n) - 1)\right) &< n \leq \\ &\leq \frac{2^{m_{\min}^{(2)}(n)}}{\sqrt{2\pi \cdot m_{\min}^{(2)}(n)}} \left(1 + \phi(m_{\min}^{(2)}(n))\right). \end{aligned}$$

Положим $\delta(m) = \log_2(1 + \phi(m))$ и возьмем логарифм по основанию 2. Получим:

$$\begin{aligned} m_{\min}^{(2)}(n) - 1 - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2(m_{\min}^{(2)}(n) - 1) + \delta(m_{\min}^{(2)}(n) - 1) &< \log_2 n \leq \\ &\leq m_{\min}^{(2)}(n) - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2 m_{\min}^{(2)}(n) + \delta(m_{\min}^{(2)}(n)), \end{aligned}$$

то есть

$$\begin{aligned} m_{\min}^{(2)}(n) - 1 - \frac{1}{2}\log_2(m_{\min}^{(2)}(n) - 1) + \delta(m_{\min}^{(2)}(n) - 1) &< \log_2 n \leq \\ &\leq m_{\min}^{(2)}(n) - \frac{1}{2}\log_2 m_{\min}^{(2)}(n) + \delta(m_{\min}^{(2)}(n)). \end{aligned}$$

Тогда

$$\begin{aligned} 1 - \frac{1}{m_{\min}^{(2)}(n)} - \frac{\log_2(m_{\min}^{(2)}(n) - 1)}{2 \cdot m_{\min}^{(2)}(n)} + \frac{\delta(m_{\min}^{(2)}(n) - 1)}{m_{\min}^{(2)}(n)} &< \frac{\log_2 n}{m_{\min}^{(2)}(n)} \leq \\ &\leq 1 - \frac{\log_2 m_{\min}^{(2)}(n)}{2 \cdot m_{\min}^{(2)}(n)} + \frac{\delta(m_{\min}^{(2)}(n))}{m_{\min}^{(2)}(n)}. \end{aligned} \quad (6)$$

Заметим, что поскольку $\lim_{m \rightarrow \infty} \phi(m) = 0$, то $\lim_{m \rightarrow \infty} \log_2(1 + \phi(m)) = 0$. Далее напомним, что $m_{\min}^{(2)}(n) \rightarrow \infty$ при $n \rightarrow \infty$. Поэтому при $n \rightarrow \infty$

$$\delta(m_{\min}^{(2)}(n)) \rightarrow 0, \quad \delta(m_{\min}^{(2)}(n) - 1) \rightarrow 0, \quad \frac{\log_2(m_{\min}^{(2)}(n) - 1)}{2 \cdot m_{\min}^{(2)}(n)} \rightarrow 0 \quad \text{и} \quad \frac{\log_2 m_{\min}^{(2)}(n)}{2 \cdot m_{\min}^{(2)}(n)} \rightarrow 0.$$

В результате из (6) получаем соотношение $\frac{\log_2 n}{m_{\min}^{(2)}(n)} = 1 + o(1)$, доказывающее утверждение.

Теперь получим нижнюю оценку величины $m_{\min}^{(k)}(n)$ при $k \geq 3$.

Утверждение 12. Пусть $k \geq 3$ – фиксированное число. Тогда существует такое n_0 , что для всех $n \geq n_0$

$$m_{\min}^{(k)}(n) > 2^{k-2} \cdot \log_2 n.$$

Доказательство. Из утверждения 9 следует, что для любой константы $C > 1$ найдется такое значение m_0 , что для всех $m > m_0$ верно неравенство

$$n_{\max}^{(k)}(m) < C \cdot 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}. \quad (7)$$

Доопределим функцию $n_{\max}^{(k)}(m)$ на все вещественные значения $x \geq 2^k$ следующим образом: $n_{\max}^{(k)}(x) = n_{\max}^{(k)}([x])$. Очевидно, что функция $n_{\max}^{(k)}(x)$ будет также неубывающей. Кроме того, для любого вещественного $x \geq 2^k$ и натурального $n_0 > k$ неравенство $n_{\max}^{(k)}(x) < n_0$ верно тогда и только тогда, когда $n_{\max}^{(k)}([x]) < n_0$. По утверждению 5 последнее неравенство эквивалентно неравенству $m_{\min}^{(k)}(n_0) > [x]$. Поскольку величина $m_{\min}^{(k)}(n)$ принимает только натуральные значения, то верны неравенства $m_{\min}^{(k)}(n_0) \geq [x] + 1 > x$. То есть, если $n_{\max}^{(k)}(x) < n_0$, то $m_{\min}^{(k)}(n_0) > x$.

Далее обозначим $\theta_m = C \cdot 2^{\frac{m}{2^{k-2}}} \cdot \sqrt{\frac{2^{k-3}}{\pi m}}$. Тогда

$$2^{k-2} \cdot \log_2 \theta_m = m + 2^{k-2} \cdot \left(\log_2 C + \frac{k-3}{2} - \frac{1}{2} \log_2 \pi - \frac{1}{2} \log_2 m \right).$$

При достаточно больших значениях m имеем:

$$\log_2 C + \frac{k-3}{2} - \frac{1}{2} \log_2 \pi - \frac{1}{2} \log_2 m < 0,$$

и поэтому $2^{k-2} \cdot \log_2 \theta_m < m$.

Поскольку функция $n_{\max}^{(k)}(m)$ – неубывающая, из (7) следует, что

$$n_{\max}^{(k)}(2^{k-2} \cdot \log_2 \theta_m) \leq n_{\max}^{(k)}(m) < \theta_m.$$

Отсюда, по доказанному выше, $m_{\min}^{(k)}(\theta_m) > 2^{k-2} \cdot \log_2 \theta_m$.

Положим $n_0(n) = 2^{k-2} \cdot \log_2 n$. Тогда $\theta_{n_0(n)} = n \cdot \frac{C}{\sqrt{2\pi \cdot \log_2 n}} < n$, начиная с достаточно большого значения n . Поскольку функция $m_{\min}^{(k)}(n)$, $n > k > 1$, является неубывающей, то

$$\begin{aligned} m_{\min}^{(k)}(n) &\geq m_{\min}^{(k)}(\theta_{n_0(n)}) > 2^{k-2} \cdot \log_2 \theta_{n_0(n)} = \\ &= n_0(n) + 2^{k-2} \cdot \left(\log_2 C + \frac{1}{2} \log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2} \log_2 n_0(n) \right) = \\ &= 2^{k-2} \cdot \log_2 n + 2^{k-2} \cdot \left(\log_2 C + \frac{1}{2} \log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2} (k-2) - \frac{1}{2} \log_2 \log_2 n \right) = \\ &= 2^{k-2} \cdot \log_2 n \left(1 + \frac{1}{\log_2 n} \cdot \left(\log_2 C + \frac{1}{2} \log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2} (k-2) - \frac{1}{2} \log_2 \log_2 n \right) \right). \end{aligned}$$

Остается заметить, что, начиная с некоторого n_0 , для всех $n \geq n_0$ верно $\frac{1}{\log_2 n} \cdot \left(\log_2 C + \frac{1}{2} \log_2 \frac{2^{k-3}}{\pi} - \frac{1}{2} (k-2) - \frac{1}{2} \log_2 \log_2 n \right) < 0$.

Список литературы

1. Глушков В.М., *Синтез цифровых автоматов*, М.: ГИФМЛ, 1962.
2. Courtois N., Meier W., “Algebraic attacks on stream ciphers with linear feedback”, EURO-CRYPT, Lect. Notes Comput. Sci., **2656**, Springer-Verlag, 2003, 346-359.
3. Логачев О.А., Сальников А.А., Смышляев С.В., Яценко В.В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2012, 583 с.
4. Dalai D., Maitra S., Sarkar S., “Basic theory in construction of Boolean functions with maximum possible annihilator immunity”, *Designs, Codes and Cryptography*, **40**:1 (2006), 41-58.
5. Jiao L., Wang M., Li Y., Liu M., “On annihilators in fewer variables: basic theory and applications”, *Chinese Journal of Electronics*, **22**:3 (2013), 489-494.
6. Глухов М.М., Шишков А.Б., *Математическая логика. Дискретные функции. Теория алгоритмов*, СПб.: Лань, 2012.
7. Горшков С.П., “Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений”, *Обозр. прикл. и пром. матем.*, **2**:3 (1995), 325-399.
8. Ролдугин П.В., Тарасов А.В., “О булевых функциях без верхних бижонктивных аналогов”, *Математические проблемы криптографии*, **4**:1 (2013), 123-140.
9. *Словарь криптографических терминов*. Под ред. Б.А. Погорелова и В.Н. Сачкова, М.: МЦНМО, 2006.