Pavel V. Roldugin, Alexey V. Tarasov, Functions without short implicents.Part I: lower estimates of weights, *Diskr. Mat.*, 2015, Volume 27, Issue 2, 94–105

Дискретная математика

том 27 выпуск 2 * 2015

УДК 519.571 DOI 10.4213/dm1327

Функции без коротких имплицент. Часть I: нижние оценки весов

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

В статье рассматриваются булевы функции от n переменных, не имеющие имплицент от k, $1 \leqslant k < n$, переменных. Получены оценки минимально возможного веса $w(n,\ k)$ таких функций. Показано, что $w(n,\ 1) = 2,\ n = 2, 3, ...,$ и $w(n,\ 2) \sim \log_2 n$ при $n \to \infty$, 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, имплиценты, 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 $f(x_1, ..., x_n)$ от n переменных, то есть $E_f = \{(\alpha_1,\ ...,\ \alpha_n) \in V_n :\ f(\alpha_1,\ ...,\ \alpha_n) = 1\}$;
- $\|f\| = |E_f|$ – 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 $f(x_1, ..., x_n)$ 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 имплиценты. 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 $\bar{h} = h \oplus 1$ – имплицента функции f. Иногда (см. [7]) имплиценту 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 имплиценты (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 имплиценты 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 имплицент, 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, $n > k \geqslant 1$. Рассмотрим класс $G_n^{(k)}$ булевых функций от n переменных, не имеющих имплицент 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 $n > k \geqslant 1$ 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 $E_f = V_n \setminus \{(\alpha_1, \ ..., \ \alpha_n)\}$, то $f\,(x_1, \ ..., \ x_n) = x_1^{\alpha_1 \oplus 1} \vee ... \vee x_n^{\alpha_n \oplus 1}$. 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 имплицент 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 $n \geqslant 2$ верно равенство $w\,(n, \ 1) = 2$.*

Доказательство. Функций веса 1 без имплицент длины 1 не существует, поскольку, если функция f принимает значение 1 на единственном наборе $(\alpha_1, \ ..., \ \alpha_n) \in V_n$, то $f\,(x_1, \ ..., \ x_n) = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$ и тогда любая функция $g = x_i^{\alpha_i}$ является имплицентой функции f. Следовательно, $w(n, 1) \geqslant 1$. Кроме того, можно прямо указать функцию веса 2 от n переменных, не имеющую имплицент длины 1 – это функция $f\,(x_1, \ ..., \ x_n) = x_1 \cdot ... \cdot x_n \vee \bar{x}_1 \cdot ... \cdot \bar{x}_n$. Действительно, для любых $i \in \overline{1, \ n}$ и $\alpha \in \{0, \ 1\}$ верно: $x_i^{\alpha} \cdot f = x_1^{\alpha} \cdot ... \cdot x_n^{\alpha} \neq x_1 \cdot ... \cdot x_n \vee \bar{x}_1 \cdot ... \cdot \bar{x}_n = f$. 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 $n \to \infty$. Для случая $k \geqslant 3$ в настоящей статье доказано существование такого n_0, что $w(n,k) > 2^{k-2} \cdot \log_2 n$ для всех $n \geqslant n_0$. Кроме того, показано, что $\min\limits_{n>k} w(n,k) = 2^k$ и, если $w(n,k) = 2^k$, то $n = k+1$.

1. Связь функций без коротких имплицент 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 имплицент, к изучению функций, не имеющих коротких элементарных имплицент.

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

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

Рассмотрим любую из элементарных дизъюнкций этой совершенной КНФ вида $K = x_{i_1}^{a_1 \oplus 1} \vee ... \vee x_{i_k}^{a_k \oplus 1}$, $(a_1, ..., a_k) \in V_n \setminus E_g$. 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 имплицент имеет наглядный комбинаторный смысл. Введем следующее определение.

Определение 1. Пусть k, $1 \leqslant k < n$, – 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 $\overrightarrow{v}$ длины k найдется строка, совпадающая с $\overrightarrow{v}$.

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 $m \geqslant 2^k \geqslant 2$. Ясно, что матрица, комбинаторно полная порядка k, $k \geqslant 2$, 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, $n \geqslant k$. 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 $n \geqslant 2k$ 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 $O\left(n^k\right)$. 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 имплицент. Матрицу, строки которой являются выполняющими векторами булевой функции f от n переменных, обозначим через $\tilde{E}_f$, то есть

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

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

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 имплиценту длины k тогда и только тогда, когда матрица $\tilde{E}_f$ не является комбинаторно полной порядка k.*

Доказательство. Рассмотрим элементарную дизъюнкцию длины $k : g = x_{i_1}^{a_1} \vee ... \vee x_{i_k}^{a_k}$. Эта дизъюнкция является имплицентой функции f тогда и только тогда, когда $f \cdot g \equiv f \cdot \left(x_{i_1}^{a_1} \vee ... \vee x_{i_k}^{a_k}\right) \equiv f$. Последнее равенство эквивалентно тому, что на всех таких векторах $(\alpha_1,\ ...,\ \alpha_n)$, что $\alpha_{i_j} = a_j \oplus 1,\ j = \overline{1,k}$, должно выполняться равенство $f(x_1,\ ...,\ x_n) = 0$. Иначе говоря, среди выполняющих векторов функции f нет таких, в которых на местах $i_1, ..., i_k$ стоят значения $a_1 \oplus 1,\ ...,\ a_k \oplus 1$ соответственно. По определению, это происходит тогда и только тогда, когда в столбцах $i_1, ..., i_k$ матрицы $\tilde{E}_f$ не содержится строк вида $(a_1 \oplus 1,\ ...,\ a_k \oplus 1)$, 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, $n > k \geqslant 1$, 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 имплицент 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 $w(n,\ k) \geqslant m_{\min}^{(k)}(n)$. 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 $m^{(k)}_{\min}(n)$ строк, что невозможно по определению величины $m^{(k)}_{\min}(n)$. В частности, отсутствие одинаковых строк означает, что $m^{(k)}_{\min}(n) \leqslant 2^n$. Но в этом случае матрицу можно рассмотреть как матрицу $\tilde{E}_f$ для функции f, задаваемой следующим способом: $E_f = \left\{\vec{A}_1,\ \vec{A}_2,\ ...,\ \vec{A}_{m^{(k)}_{\min}(n)}\right\}$, где $\vec{A}_i$ – строки матрицы A. Функция f от n переменных веса $m^{(k)}_{\min}(n)$ не имеет имплицент в силу утверждения 3, и поэтому получаем обратное неравенство $w(n,\ k) \leqslant m^{(k)}_{\min}(n)$, 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, $n > k \geqslant 1$, верно неравенство*

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

Двойственной задачей к вычислению $m^{(k)}_{\min}(n)$ является нахождение для фиксированного числа строк m максимального значения $n^{(k)}_{\max}(m)$ числа столбцов, при котором существует комбинаторно полная матрица размера $m \times n^{(k)}_{\max}(m)$ 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 $m^{(k)}_{\min}(n)$ определено при всех $k \geqslant 1$; значение же величины $n^{(k)}_{\max}(m)$ определяется только при $k > 1$, поскольку при $k = 1$ в качестве комбинаторно полной матрицы порядка 1 можно взять матрицу $\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \end{pmatrix}$, имеющую всего две строки, но произвольное число столбцов. Поэтому далее будем рассматривать только случай $k > 1$.

При фиксированном $k > 1$ значение $n^{(k)}_{\max}(m)$ определено при всех $m \geqslant 2^k$. Функция $n^{(k)}_{\max}(m)$ является неубывающей, то есть $n^{(k)}_{\max}(m) \leqslant n^{(k)}_{\max}(m+1)$, поскольку, как отмечалось выше, в комбинаторно полную матрицу можно добавлять любые строки. Однако не доказано, что при любом фиксированном k функция $n^{(k)}_{\max}(m)$ 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 $m^{(k)}_{\min}(n)$, $n > k > 1$, является неубывающей.

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

Связь между значениями $m^{(k)}_{\min}(n)$ и $n^{(k)}_{\max}(m)$ 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 $m_0 \geqslant 2^k + 1$ верны неравенства*

$$n^{(k)}_{\max}(m_0 - 1) < n_0 \leqslant n^{(k)}_{\max}(m_0),$$

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

2) *верно неравенство*

$$n_0 \leqslant n^{(k)}_{\max}\left(2^k\right),$$

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

Доказательство. Поскольку, как показано выше, область значений функции $n^{(k)}_{\max}(m)$, $m \geqslant 4$, $k > 1$, ограничена снизу значением $n^{(k)}_{\max}\left(2^k\right)$ 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 $m_0 \geqslant 2^k + 1$, что $n^{(k)}_{\max}(m_0 - 1) < n_0 \leqslant n^{(k)}_{\max}(m_0)$. Неравенство $n_0 \leqslant n^{(k)}_{\max}(m_0)$ означает, что существует комбинаторно полная матрица порядка k и размера $m_0 \times n_0$. Отсюда следует, что $m^{(k)}_{\min}(n_0) \leqslant m_0$. Докажем, что $m^{(k)}_{\min}(n_0) = m_0$. От противного: пусть $m^{(k)}_{\min}(n_0) = m_0'$ 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 $n_0 \leqslant n^{(k)}_{\max}(m_0 - 1)$, что противоречит условию. Второй случай очевиден.

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

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

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 $n^{(k)}_{\max}(m)$, далее на основе утверждений 4 или 5, выводятся нижние оценки величины $m^{(k)}_{\min}(n)$, которые, в силу следствия 1 утверждения 3, являются нижними оценками для $w(n, k)$.

2. Верхние оценки величины $n^{(k)}_{\max}(m)$**.** 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* $n^{(k)}_{\max}\left(2^k\right) = k + 1$.

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 $\left\{\left(\alpha_1,\ ...,\ \alpha_k,\ \beta_{(\alpha_1,\ ...,\ \alpha_k)}\right) :\ (\alpha_1,\ ...,\ \alpha_k) \in V_k\right\}$.

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

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

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 $1,\ 2,\ ...,\ i-1,\ i+1,\ ...,\ k,\ k+1$. 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 связен и двудолен: одна из долей образована вершинами $(\alpha_1,\ ...,\ \alpha_k)$ четного веса, другая – нечетного веса.

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

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

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 $\left(B_1^{\downarrow},\ ...,\ B_k^{\downarrow},\ B_{k+1}^{\downarrow}\right)$ и $\left(B_1^{\downarrow},\ ...,\ B_k^{\downarrow},\ B_{k+2}^{\downarrow}\right)$, 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 $n_{\max}\left(2^k\right) = k+1$.

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

$$n_{\max}^{(2)}(m) = \begin{cases} \dfrac{1}{2} \cdot \dbinom{2r}{r},\ m = 2r, \\ \dbinom{2r}{r-1},\ m = 2r+1, \end{cases} \quad m \geqslant 4.$$

Далее рассмотрим случай $k \geqslant 3$.

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

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

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

считать, что в первом столбце первые t элементов равны 0, а последние $m-t$ равны единице, $2^{k-1} \leqslant t \leqslant m - 2^{k-1}$.

Рассмотрим подматрицы A_0 и A_1, составленные, соответственно, из первых t и последних $m-t$ строк и $n-1$ последних столбцов матрицы A (рис. 1).

$$A = \begin{array}{c} \\ t \\ m-t \end{array} \begin{array}{c} \overbrace{}^{n-1} \\ \left(\begin{array}{c|c} 0 & \\ \vdots & A_0 \\ 0 & \\ \hline 1 & \\ \vdots & A_1 \\ 1 & \end{array} \right) \end{array}.$$

Рис. 1

Поскольку A – комбинаторно полная матрица порядка k, то, в частности, для всякого набора из k столбцов вида $A^{\downarrow}_1,\ A^{\downarrow}_{i_1},\ ...,\ A^{\downarrow}_{i_{k-1}}$, $1 < i_1 < i_2 < ... < i_{k-1} \leqslant n$, в этих столбцах встречается любая комбинация $(a_1,\ ...,\ a_k) \in V_k$. При этом комбинации вида $(0,\ a_2,\ ...,\ a_k)$ находятся в одной из первых t строк, а комбинации вида $(1,\ a_2,\ ...,\ a_k)$ – в одной из строк с номерами $t+1, \ldots, m$.

Это означает, что для всякого набора из $k-1$ столбцов вида $A^{\downarrow}_{i_1},\ ...,\ A^{\downarrow}_{i_{k-1}}, 1 < i_1 < i_2 < ... < i_{k-1} \leqslant n$, в этих столбцах любая комбинация $(a_2,\ ...,\ a_k) \in V_{k-1}$ встречается как минимум дважды: в одной из первых t строк и в одной из последних $m-t$ строк. Следовательно, обе матрицы A_0 и A_1 являются комбинаторно полными порядка $k-1$.

Каждая из этих матриц содержит по $n-1$ столбцов, следовательно, $n-1 \leqslant n^{(k-1)}_{\max}(t)$ и $n-1 \leqslant n^{(k-1)}_{\max}(m-t)$, то есть верно неравенство

$$n \leqslant \min\left\{ n^{(k-1)}_{\max}(t),\ n^{(k-1)}_{\max}(m-t) \right\} + 1.$$

Поскольку, как отмечалось выше, функция $n^{(k)}_{\max}(m)$ – неубывающая, и либо $t \leqslant \left[\frac{m}{2}\right]$, либо $m-t \leqslant \left[\frac{m}{2}\right]$, то $\min\left\{ n^{(k-1)}_{\max}(t),\ n^{(k-1)}_{\max}(m-t) \right\} \leqslant n^{(k-1)}_{\max}\left(\left[\frac{m}{2}\right]\right)$. Получаем искомое неравенство

$$n^{(k)}_{\max}(m) \leqslant n^{(k-1)}_{\max}\left(\left[\frac{m}{2}\right]\right) + 1.$$

Из полученного неравенства можно вывести следующую оценку, использующую на функцию $n^{(2)}_{\max}(m)$.

Утверждение 8. *Пусть $k \geqslant 3$ и $m \geqslant 2^k$. Тогда*

$$n^{(k)}_{\max}(m) \leqslant n^{(2)}_{\max}\left(\left[\frac{m}{2^{k-2}}\right]\right) + k - 2.$$

Доказательство. Поскольку $\left[\frac{[m/2]}{2}\right] = \left[\frac{m}{4}\right]$, то из утверждения 7 получаем, что

$$n^{(k)}_{\max}(m) \leqslant n^{(k-2)}_{\max}\left(\left[\frac{m}{4}\right]\right) + 2.$$

Далее итеративно получаем, что для произвольного $r = 1,\ 2,\ ...,\ k-2$ выполняется неравенство

$$n^{(k)}_{\max}(m) \leqslant n^{(k-r)}_{\max}\left(\left[\frac{m}{2^r}\right]\right) + r.$$

В итоге при $r = k - 2$ имеем:

$$n^{(k)}_{\max}(m) \leqslant n^{(2)}_{\max}\left(\left[\frac{m}{2^{k-2}}\right]\right) + k - 2.$$

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

Утверждение 9. *Пусть $k \geqslant 3$ – фиксированное число. Тогда при $m \to \infty$*

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

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

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

Подставляя это соотношение в оценку из утверждения 8, получаем

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

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

$$n^{(k)}_{\max}(m) \leqslant \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{2\pi\left(\frac{m}{2^{k-2}} - 1\right)}} \cdot (1 + \phi(m)) + k - 2 \leqslant$$

$$\leqslant \sqrt{\frac{2^{k-3}}{\pi}} \cdot \frac{2^{\frac{m}{2^{k-2}}}}{\sqrt{m}} \cdot \left(\left(1 - \frac{2^{k-2}}{m}\right)^{-1/2} \cdot (1 + \phi(m)) + (k-2) \cdot \sqrt{\frac{\pi}{2^{k-3}}} \cdot \frac{\sqrt{m}}{2^{\frac{m}{2^{k-2}}}}\right). \tag{4}$$

Поскольку $k \geqslant 3$, то $\sqrt[2^{k-2}]{2} > 1$, следовательно, $\frac{\sqrt{m}}{\left(\sqrt[2^{k-2}]{2}\right)^m} \underset{m\to\infty}{\to} 0$. Кроме того, $\frac{2^{k-2}}{m} \underset{m\to\infty}{\to} 0$. 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 $m \to \infty$.

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

Начнем с равенства $n^{(k)}_{\max}\left(2^k\right) = k + 1, k > 1$, 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 $(\alpha_1,\, ...,\, \alpha_{k+1}) \in E_f$ справедливо равенство $\alpha_1 \oplus ... \oplus \alpha_k \oplus \nu = \alpha_{k+1}$ при некотором фиксированном $\nu \in \{0,\, 1\}$. Очевидно, что таких функции всего две: $f(x_1,\, ...,\, x_{k+1}) = x_1 \oplus ... \oplus x_{k+1}$ и $f(x_1,\, ...,\, x_{k+1}) = x_1 \oplus ... \oplus x_{k+1} \oplus 1$. Таким образом, доказано следующее утверждение.

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

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 $f(x_1, \ldots, x_n)$ 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 имплицент от $n-1$ переменных" эквивалентно выражению "у функции от n переменных нет имплицент 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 $f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ и $f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n \oplus 1$, имеет имплиценту от меньшего числа переменных.*

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

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

Утверждение 11. *При $n \to \infty$ верно соотношение*

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

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

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

$$n^{(2)}_{\max}\left(m^{(2)}_{\min}(n) - 1\right) < n \leqslant n^{(2)}_{\max}\left(m^{(2)}_{\min}(n)\right). \tag{5}$$

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

$$\frac{2^{m^{(2)}_{\min}(n)-1}}{\sqrt{2\pi \cdot \left(m^{(2)}_{\min}(n) - 1\right)}} \left(1 + \phi\left(m^{(2)}_{\min}(n) - 1\right)\right) < n \leqslant$$

$$\leqslant \frac{2^{m^{(2)}_{\min}(n)}}{\sqrt{2\pi \cdot m^{(2)}_{\min}(n)}} \left(1 + \phi\left(m^{(2)}_{\min}(n)\right)\right).$$

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

$$m^{(2)}_{\min}(n) - 1 - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2\left(m^{(2)}_{\min}(n)-1\right) + \delta\left(m^{(2)}_{\min}(n)-1\right) < \log_2 n \leqslant$$

$$\leqslant m^{(2)}_{\min}(n) - \frac{1}{2}\log_2 2\pi - \frac{1}{2}\log_2 m^{(2)}_{\min}(n) + \delta\left(m^{(2)}_{\min}(n)\right),$$

то есть

$$m^{(2)}_{\min}(n) - 1 - \tfrac{1}{2}\log_2\left(m^{(2)}_{\min}(n)-1\right) + \delta\left(m^{(2)}_{\min}(n)-1\right) < \log_2 n \leqslant$$

$$\leqslant m^{(2)}_{\min}(n) - \tfrac{1}{2}\log_2 m^{(2)}_{\min}(n) + \delta\left(m^{(2)}_{\min}(n)\right).$$

Тогда

$$1 - \frac{1}{m^{(2)}_{\min}(n)} - \frac{\log_2\left(m^{(2)}_{\min}(n)-1\right)}{2\cdot m^{(2)}_{\min}(n)} + \frac{\delta\left(m^{(2)}_{\min}(n)-1\right)}{m^{(2)}_{\min}(n)} < \frac{\log_2 n}{m^{(2)}_{\min}(n)} \leqslant$$

$$\leqslant 1 - \frac{\log_2 m^{(2)}_{\min}(n)}{2\cdot m^{(2)}_{\min}(n)} + \frac{\delta\left(m^{(2)}_{\min}(n)\right)}{m^{(2)}_{\min}(n)}. \tag{6}$$

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

$$\delta\left(m^{(2)}_{\min}(n)\right) \to 0,\ \delta\left(m^{(2)}_{\min}(n)-1\right) \to 0,\ \frac{\log_2\left(m^{(2)}_{\min}(n)-1\right)}{2\cdot m^{(2)}_{\min}(n)} \to 0 \text{ и } \frac{\log_2 m^{(2)}_{\min}(n)}{2\cdot m^{(2)}_{\min}(n)} \to 0.$$

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

Теперь получим нижнюю оценку величины $m^{(k)}_{\min}(n)$ при $k \geqslant 3$.

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

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

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

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

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

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 $n^{(k)}_{\max}(m)$ – неубывающая, из (7) следует, что

$$n^{(k)}_{\max}\left(2^{k-2}\cdot\log_2\theta_m\right) \leqslant n^{(k)}_{\max}(m) < \theta_m.$$

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

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 $m^{(k)}_{\min}(n)$, $n > k > 1$, является неубывающей, то

$$m^{(k)}_{\min}(n) \geqslant m^{(k)}_{\min}\left(\theta_{n_0(n)}\right) > 2^{k-2}\cdot\log_2\theta_{n_0(n)} =$$

$$= n_0(n) + 2^{k-2}\cdot\left(\log_2 C + \frac{1}{2}\log_2\frac{2^{k-3}}{\pi} - \frac{1}{2}\log_2 n_0(n)\right) =$$

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

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

Остается заметить, что, начиная с некоторого n_0, для всех $n \geqslant n_0$ 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", EUROCRYPT, Lect. Notes Comput. Sci., **2656**, Springer-Verlag, 2003, 346-359.
3. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко 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 биюнктивных 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.

Статья поступила 27.01.2015.