Math-Net.Ru

Общероссийский математический портал

В. Г. Никонов, О числе существенных переменных равновероятной булевой функции с фиксированным количеством элементарных конъюнкций в ДНФ, *Матем. вопр. криптогр.*, 2011, том 2, выпуск 4, 37–47

DOI: <https://doi.org/10.4213/mvk42>

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: 54.198.67.100

26 апреля 2023 г., 13:28:08

УДК 519.714.83

О числе существенных переменных равновероятной булевой функции с фиксированным количеством элементарных конъюнкций в ДНФ

В. Г. Никонов

Академия криптографии Российской Федерации, Москва

Получено 23.VI.2010

Получены верхние и нижние оценки числа $n(k)$ существенных переменных равновероятной булевой функции, заданной в виде ДНФ с помощью k элементарных конъюнкций. Ограниченность числа $n(k)$ для любого k была доказана автором ранее. Равновероятные булевы функции представляют первостепенный интерес для криптографических приложений, а их представлению в виде ДНФ соответствует реализация на современной элементной базе, в частности, с помощью программируемых логических матриц.

Ключевые слова: булева функция, дизъюнктивная нормальная форма, числа Фибоначчи

On the number of significant variables of balanced Boolean function with the fixed number of elementary conjunctions in its DNF

V. G. Nikonov

Academy of Cryptography of Russian Federation, Moscow

Abstract. The upper and lower bounds for the number $n(k)$ of significant variables of balanced Boolean function represented by k elementary conjunction are obtained. The boundedness of $n(k)$ for every k was proved by the author previously. Balanced Boolean functions are very important for cryptography; their DNF representations correspond to realizations by circuits, in particular, by programmable logical matrices.

Key words: Boolean function, DNF (disjunctive normal form), Fibonacci numbers

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 4, pp. 37–47 (Russian).

Представление булевых функций в виде ДНФ используется в задачах анализа и синтеза узлов переработки информации (см. [1–8]), особый интерес представляет задание в виде ДНФ равновероятных функций.

При задании булевой функции в виде ДНФ

$$f(x_1, \dots, x_n) = q_1 \vee \dots \vee q_k \quad (1)$$

каждая элементарная конъюнкция

$$q_i = x_{i_1}^{\varepsilon_{i_1}} \cdot \dots \cdot x_{i_{l(i)}}^{\varepsilon_{i_{l(i)}}}$$

определяет в n -мерном единичном кубе V_n подкуб Q_i размерности $n - l(i)$, покрывающий множество единичных вершин $A_f \subseteq V_n$, все вершины которого удовлетворяют условиям

$$\begin{aligned} x_{i_1} &= \varepsilon_{i_1}, \\ &\vdots \\ x_{i_{l(i)}} &= \varepsilon_{i_{l(i)}}. \end{aligned}$$

Произведению

$$q_i \cdot q_j = x_{i_1}^{\varepsilon_{i_1}} \cdot \dots \cdot x_{i_{l(i)}}^{\varepsilon_{i_{l(i)}}} \cdot x_{j_1}^{\varepsilon_{j_1}} \cdot \dots \cdot x_{j_{l(j)}}^{\varepsilon_{j_{l(j)}}} \quad (2)$$

двух элементарных конъюнкций

$$q_i = x_{i_1}^{\varepsilon_{i_1}} \cdot \dots \cdot x_{i_{l(i)}}^{\varepsilon_{i_{l(i)}}} \text{ и } q_j = x_{j_1}^{\varepsilon_{j_1}} \cdot \dots \cdot x_{j_{l(j)}}^{\varepsilon_{j_{l(j)}}} \quad (3)$$

соответствует подкуб $Q_{ij} = Q_i \cap Q_j$ размерности $n - v$, где v — число различных переменных в записи (2). Произведение (2) задает пустой подкуб, $Q_{ij} = Q_i \cap Q_j = \emptyset$ (т. е. подкубы Q_i , Q_j не пересекаются) тогда и только тогда, когда некоторая переменная входит в задание одной элементарной конъюнкции (3) в прямом, а в задание другой — в инверсном виде.

Вес функции $f(x_1, \dots, x_n)$ $\|f(x_1, \dots, x_n)\| = |A_f|$ вычисляются по формуле включения–исключения:

$$\begin{aligned} \|f(x_1, \dots, x_n)\| &= |A_f| = |Q_1| + \dots + |Q_k| - |Q_1 \cap Q_2| - \dots - |Q_{k-1} \cap Q_k| + \\ &+ |Q_1 \cap Q_2 \cap Q_3| + \dots + (-1)^k |Q_1 \cap \dots \cap Q_k|, \end{aligned} \quad (4)$$

где каждое непустое пересечение подкубов $Q_{i_1} \cap \dots \cap Q_{i_t}$ задает некоторый подкуб $Q_{i_1 \dots i_t}$ и, следовательно, каждое слагаемое в правой части формулы (4) равно $\pm 2^d$ или 0.

В статье [1] рассматривались равновероятные булевы функции $f(x_1, \dots, x_n)$, представленные в виде ДНФ с помощью k элементарных конъюнкций, для которых левая часть в равенстве (4) равна $\|f(x_1, \dots, x_n)\| = 2^{n-1}$.

В статье [1] доказано утверждение.

Теорема 1. *Равновероятная булева функция с фиксированным числом элементарных конъюнкций в своем представлении в виде ДНФ (1) существенно зависит от ограниченного числа переменных.*

Доказательство теоремы основывалось на детальном анализе строения равновероятных функций, заданных с помощью k элементарных конъюнкций, из которого следовало, что в задании функции не может участвовать элементарная конъюнкция, содержащая сколь угодно много переменных. Следовательно, для любого k существует число $n(k)$, равное максимальному количеству переменных, от которых может зависеть равновероятная функция, представленная в виде ДНФ с использованием k элементарных конъюнкций. Отсюда же вытекает, что класс $F(k)$ равновероятных булевых функций с фиксированным количеством k элементарных конъюнкций в ДНФ конечен и все составляющие его функции могут быть, в принципе, перечислены.

Данная статья посвящена нахождению оценки величины $n(k)$ с помощью конструктивного подхода, основанного на построении специальных классов булевых функций.

Лемма 1. *Булева функция n переменных*

$$f_2(x_1, \dots, x_n) = x_1 x_2 \vee x_3 x_4 \vee \bar{x}_1 \bar{x}_3 x_5 \cdot f_1(x_6, \dots, x_n) \quad (5)$$

является равновероятной тогда и только тогда, когда равновероятной является функция $f_1(x_6, \dots, x_n)$.

Доказательство леммы проводится непосредственным вычислением веса функции.

Через $r_1(k)$ обозначим число существенных переменных равновероятных функций класса $F_1(k)$ вида (5) с k элементарными конъюнкциями.

Из леммы 1 следует неравенство

$$r_1(k+2) \geq r_1(k) + 5,$$

а с учетом того, что $n(1)=1$, $n(2)=3$ — теорема 2.

Теорема 2. *Справедлива оценка*

$$n(k) \geq r_1(k) = \begin{cases} 5m+1, & \text{если } k = 2m+1, \\ 5m-2, & \text{если } k = 2m. \end{cases} \quad (6)$$

Оценка (6) может быть улучшена.

Для получения искомой оценки в классе $F(k)$ выделим новый подкласс $F_2(k) \subset F(k)$, включив в него при $k=1, 2$ следующие функции:

$$\begin{aligned} k=1, \quad f^{(1)} &= x_1; \\ k=2, \quad f^{(2)} &= x_1 x_2 \vee \overline{x_1 x_3}; \end{aligned}$$

при $k \geq 3$ — функции вида

$$f^{(k)} = f_1^{(k)} \vee f_2^{(k)} \vee f_3^{(k)} \vee \dots \vee f_k^{(k)},$$

где $f_i^{(k)}$ — элементарные конъюнкции, $f_1^{(k)} = x_1 x_2$, $f_2^{(k)} = x_3 x_4$, удовлетворяющие условиям:

$$1. \left| A_{f_i^{(k)}} \cap A_{f_{i+1}^{(k)}} \right| = \left| A_{f_{i+2}^{(k)}} \right|,$$

$A_{f_j^{(k)}}$ — множество, на котором $f_j^{(k)} = 1$, $\left| A_{f_{k-1}^{(k)}} \cap A_{f_k^{(k)}} \right| = 0$;

$$2. \left| A_{f_{i_1}^{(k)}} \cap A_{f_{i_2}^{(k)}} \right| = 0 \quad \text{при } |i_1 - i_2| > 1, \quad i_1, \quad i_2 = 1, \dots, k.$$

Прежде всего отметим, что класс функций $F_2(k)$, в исследовании которого принимал также участие Никитин Н. А., является подклассом класса $F(k)$. Действительно, вес функции $f^{(k)}$ при $k \geq 3$ вычисляется по формуле включения–исключения и равен

$$\begin{aligned} \|f^{(k)}\| &= \left| A_{f^{(k)}} \right| = \left| A_{f_1^{(k)}} \right| + \dots + \left| A_{f_k^{(k)}} \right| - \left| A_{f_1^{(k)}} \cap A_{f_2^{(k)}} \right| - \dots - \left| A_{f_{k-2}^{(k)}} \cap A_{f_{k-1}^{(k)}} \right| = \\ &= \left| A_{f_1^{(k)}} \right| + \dots + \left| A_{f_k^{(k)}} \right| - \left| A_{f_3^{(k)}} \right| - \dots - \left| A_{f_k^{(k)}} \right| = \left| A_{f_1^{(k)}} \right| + \left| A_{f_2^{(k)}} \right| = 2^{n-1}, \end{aligned}$$

так как $f_1^{(k)} = x_1 x_2$, $f_2^{(k)} = x_3 x_4$, то есть функции $f^{(k)}$ — равновероятные (при $k=1, 2$ равновероятность $f^{(1)}$, $f^{(2)}$ очевидна) и $F_2(k) \subset F(k)$.

Введем понятие семейства функций, важное для описания строения функций с фиксированной сложностью представления в ДНФ.

Рассмотрим произвольную функцию, заданную в виде ДНФ,

$$f(x_1, \dots, x_n) = q_1 \vee \dots \vee q_k,$$

где $q_j = x_{j_1}^{\varepsilon_{j_1}} \dots x_{j_t(j)}^{\varepsilon_{j_t(j)}}$.

Для любого подмножества конъюнкций $q_{i_1}, \dots, q_{i_t}$, $t = 1, \dots, k$, назовём его длиной $l(q_{i_1}, \dots, q_{i_t})$ число различных переменных (в прямом или инверсном виде) в конъюнкции

$$q_{i_1 \dots i_t} = q_{i_1} \cdot \dots \cdot q_{i_t},$$

если $q_{i_1 \dots i_t} \neq 0$, и 0, если $q_{i_1 \dots i_t} = 0$.

Определение 1. Отождествление переменных $x_\mu^\varepsilon = x_\nu$, $x_\mu, x_\nu \in (x_1, x_2, \dots, x_{n+1}, \dots)$, $\varepsilon = 0, 1$, назовем *допустимым* для функции $f(x_1, \dots, x_n)$, если у редуцированной функции

$$f\left(x_1, \dots, x_n \middle/ x_\mu^\varepsilon = x_\nu\right) = q_1(x_\mu^\varepsilon = x_\nu) \vee \dots \vee q_k(x_\mu^\varepsilon = x_\nu)$$

и у исходной функции для всех подмножеств элементарных конъюнкций $q_{i_1}, \dots, q_{i_t}$ совпадают длины

$$l(q_{i_1}(x_\mu^\varepsilon = x_\nu), \dots, q_{i_t}(x_\mu^\varepsilon = x_\nu)) = l(q_{i_1}, \dots, q_{i_t}).$$

Легко проверить, что допустимое отождествление переменных преобразует равновероятную функцию в равновероятную и, более того, не выводит функцию, принадлежащую классу $F_2(k)$, за рамки этого класса.

Определение 2. Семейством, порожденным функцией $f(x_1, \dots, x_n)$, назовем множество всех функций, полученных из $f(x_1, \dots, x_n)$ с помощью последовательности допустимых отождествлений переменных.

Из определения 2 вытекает, что вместе с любой функцией семейство содержит и все с ней однотипные как следствие двух допустимых отождествлений, $x_\mu = x_{n+1}$, $x_{n+1} = x_\nu^\varepsilon$.

Группировка функций в семейства представляется удобным приемом описания строения различных классов функций, в том числе — равновероятных. Семейства могут быть заданы одной ДНФ и являются более крупным объединением функций, чем типы. Внутри семейства все функции имеют фиксированное число элементарных конъюнкций в ДНФ, что важно для пересчета функций с ограниченной сложностью представления.

Вернемся к изучению класса $F_2(k)$ и через $r_2(k)$ обозначим максимальное число существенных переменных функций, входящих в класс $F_2(k)$.

Теорема 3. *Справедливы равенства $r_2(1)=1$, $r_2(2)=3$, а при $k \geq 3$*

$$r_2(k) \geq 2 \sum_{i=1}^k h(i) - \frac{(k-2)(k-3)}{2} - c(k), \quad (7)$$

где $h(i)$ — число Фибоначчи: $h(i+2)=h(i+1)+h(i)$ при $h(1)=1$, $h(2)=1$; $c(k)$ — целочисленная функция, принимающая значения $c(3)=2$, $c(4)=3$, $c(k)=4$ при $k \geq 5$.

Доказательство. Построим семейство Φ_k при $k \geq 5$, порождающую функцию которого

$$\varphi_k = q_1 \vee \dots \vee q_k$$

определим элементарными конъюнкциями

$$\begin{aligned} q_1 &= y_{11}y_{12}, \\ q_2 &= y_{21}y_{22}, \\ q_3 &= y_{31}y_{32}y_{33}y_{34}, \\ &\vdots \\ q_t &= y_{t1}y_{t2} \dots y_{tm_t}, \\ &\vdots \\ q_k &= y_{k1}y_{k2} \dots y_{km_k}, \end{aligned} \quad (8)$$

где $m_1=2$, $m_2=2$ и $m_j = m_{j-1} + m_{j-2}$ при $j \geq 3$, переменные y_{ti} удовлетворяют условиям

$$\begin{aligned} y_{t1} &= \begin{cases} \bar{y}_{11}, & \text{если } t \text{ нечетное,} \\ \bar{y}_{12}, & \text{если } t \text{ четное,} \end{cases} \\ y_{t2} &= \begin{cases} \bar{y}_{22}, & \text{если } t \text{ нечетное,} \\ \bar{y}_{21}, & \text{если } t \text{ четное,} \end{cases} \\ y_{ti} &= \begin{cases} \bar{y}_{ii}, & \text{если } t \text{ нечетное,} \\ \bar{y}_{i-i}, & \text{если } t \text{ четное;} \end{cases} \quad 3 \leq i \leq t-2, \quad t \leq k-1, \end{aligned} \quad (9)$$

$$\begin{aligned}
y_{k1} &= y_{11}, \\
y_{k2} &= \bar{y}_{12}, \\
y_{k3} &= \bar{y}_{21}, \\
y_{k4} &= \bar{y}_{22},
\end{aligned} \tag{10}$$

а переменные, не вошедшие в условия (9), (10), — независимые.

Доопределим Φ_k и при $k=3, 4$, задавая порождающие функции φ_3 и φ_4 в виде

$$\varphi_3 = y_{11}y_{12} \vee y_{21}y_{22} \vee \bar{y}_{11}\bar{y}_{21}y_{33}y_{34}, \tag{11}$$

$$\varphi_4 = y_{11}y_{12} \vee y_{21}y_{22} \vee \bar{y}_{11}y_{32}y_{33}y_{34} \vee y_{11}\bar{y}_{12}\bar{y}_{22}y_{44}y_{45}y_{46}. \tag{12}$$

При любом $k \geq 3$ порождающая функция φ_k принадлежит классу $F_2(k)$, в чем нетрудно убедиться непосредственной проверкой. Следовательно, всё семейство Φ_k содержится в классе $F_2(k)$.

Количество $r_2(k)$ существенных переменных порождающей функции φ_k складывается из общего числа переменных, введенных для записи конъюнкций (8): $\delta_1(k) = \sum_{i=1}^k m_i = 2 \sum_{i=1}^k h(i)$, за вычетом количества переменных, отождествляемых равенствами (9),

$$\delta_2(k) = \sum_{\theta=1}^{k-3} \theta = \frac{(k-2)(k-3)}{2} \tag{13}$$

и количества $c(k)$ переменных, зафиксированных равенствами (10):

$$r_2(k) = \delta_1(k) - \delta_2(k) - c(k). \tag{14}$$

При $k \geq 5$ значение $c(k)$ равно 4, из записи функций (11) и (12) следует, что при $k=3, 4$ формула (14) справедлива, если положить $c(3)=2$ и $c(4)=3$.

Из равенств (13), (14) и следует оценка (7). Теорема доказана.

Следствие 1. Справедливо неравенство

$$n(k) \geq 2 \sum_{i=1}^k h(i) - \frac{(k-2)(k-3)}{2} - c(k). \tag{15}$$

Отметим, что оценка (15) значения $n(k)$ при $k \geq 4$ превосходит (6), то есть $r_2(k) \geq r_1(k)$. Это можно доказать путем индукции, предположив, что

$r_2(k) \geq r_1(k)$ для всех $k \leq k_0$ при $r_2(1) = r_1(1)$, $r_2(2) = r_1(2)$ и рассмотрев разность $r_2(k+1) \geq r_1(k+1)$. Учитывая, что $c(k+1) \leq c(k) + 1$ и $r_1(k+1) \leq r_1(k) + 3$ получаем:

$$\begin{aligned} r_2(k+1) - r_1(k+1) &\geq r_2(k) - r_1(k) + 2h(k+1) - \frac{(k-1)(k-2)}{2} + \\ &\quad + \frac{(k-2)(k-3)}{2} - c(k+1) + c(k) - 3 \geq \\ &\geq r_2(k) - r_1(k) + 2 \cdot h(k+1) - k - 2 \geq 2 \cdot h(k+1) - k - 2 \end{aligned}$$

(используем предположение индукции: $r_2(k) \geq r_1(k)$).

Далее, так как при $k \geq 4$

$$h(k+1) = \sum_{l=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k-l}{l} = k-1 + \sum_{l=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k-l}{l} + 1,$$

то

$$r_2(k+1) - r_1(k+1) \geq 2 \cdot h(k+1) - k - 2 = k - 2 + 2 \cdot \sum_{l=2}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k-l}{l} \geq 0,$$

которое выполняется при любом $k \geq 4$, то есть $r_2(k+1) \geq r_1(k+1)$.

После исследования максимального числа $n(k)$ существенных переменных равновероятной булевой функции, заданной с помощью k элементарных конъюнкций, обратимся к рассмотрению минимального числа $m(k)$ существенных переменных функций из класса $F(k)$. В следующих теоремах находится это число и указываются функции, которые имеют минимальное число существенных переменных.

Теорема 4. Если равновероятная булева функция f представима в виде кратчайшей ДНФ (КДНФ) $k = 2^s$ элементарными конъюнкциями

$$f = q_1 \vee q_2 \vee \dots \vee q_{2^s}, \quad (16)$$

то $m(k) = s + 1$.

Доказательство. Допустим, что f зависит существенно от $l < s + 1$ переменных, тогда, так как f — равновероятная функция,

$$\|f(x_1, \dots, x_l)\| = 2^{l-1} < 2^s;$$

следовательно, f представима в виде ДНФ с менее чем 2^s конъюнкциями, а именно:

$$f(x_1, \dots, x_l) = \bigvee_{f(\varepsilon_1 \dots \varepsilon_l)=1} x_1^{\varepsilon_1} \dots x_l^{\varepsilon_l}.$$

Это противоречит тому, что (16) является кратчайшей ДНФ для функции f , следовательно, $m(k) \geq s+1$.

Напомним, что каноническим индексом булевой функции $f(x_1, \dots, x_n)$ в работах [6, 7, 8] названо число элементарных конъюнкций в кратчайшей ДНФ функции $f(x_1, \dots, x_n)$.

Рассмотрим линейную функцию

$$f_k(x_1, \dots, x_{s+1}) = x_1 \oplus x_2 \oplus \dots \oplus x_{s+1}.$$

Как известно, функция f представима в КДНФ с помощью 2^s элементарных конъюнкций, то есть имеет канонический индекс $k = 2^s$ (см. [6, 7, 8]).

$$f_{2^s}(x_1, \dots, x_{s+1}) = \bigvee_{f(\varepsilon_1 \dots \varepsilon_{s+1})=1} x_1^{\varepsilon_1} \dots x_{s+1}^{\varepsilon_{s+1}} = q_1 \vee \dots \vee q_{2^s}.$$

Отсюда получаем $m(k) \leq s+1$ и окончательно $m(k) = s+1$. Теорема доказана.

Теорема 5. Если представление функции f в КДНФ имеет вид

$$f = q_1 \vee q_2 \vee \dots \vee q_k, \quad (17)$$

где $2^s < k \leq 2^{s+1}$, то $m(k) = s+1$.

Доказательство. Предположим, что функция f зависит существенно от $l \leq s+1$ переменных. Тогда, так как f — равновероятная функция, $\|f(x_1, \dots, x_l)\| = 2^{l-1} \leq 2^s < k$; следовательно, f представима в виде ДНФ с менее чем k конъюнкциями, что противоречит представлению f в виде (17). Отсюда получаем $m(k) \geq s+2$.

Рассмотрим последовательность функций φ_k , устроенных следующим образом:

1) если $k = 2^{s+1}$, то $\varphi_k(x_1, \dots, x_{s+2}) = f_k = f_{2^s}$;

2) если $2^s < k < 2^{s+1}$, то

$$\varphi_k(x_1, \dots, x_{s+2}) = x_{s+2} f_{2^s}(x_1, \dots, x_{s+1}) \vee \bar{x}_{s+2} \varphi_{(k-2^s)}(x_1, \dots, x_l),$$

где $l < s+2$, так как $k - 2^s < 2^s$.

Докажем по индукции, что φ_k — равновероятные функции. Действительно, $\varphi_1 = x_1$, $\varphi_2 = f_2 = x_1 \bar{x}_2 \vee \bar{x}_1 x_2$ — равновероятны. Предположим, что для всех $l < k$ функции φ_l равновероятны, тогда, так как $(k - 2^s) < k$,

$$\|\varphi_k(x_1, \dots, x_{s+2})\| = \|f_{2^s}\| + \|\varphi_{(k-2^s)}(x_1, \dots, x_l)\| \cdot 2^{s+1-l} = 2^s + 2^{l-1} \cdot 2^{s+1-l} = 2^{s+1}.$$

Следовательно, функция $\varphi_k(x_1, \dots, x_{s+2})$ — равновероятна и представима в ДНФ k конъюнкциями. Докажем по индукции, что это представление есть КДНФ, то есть всегда найдется существенная система вершин (ССВ) для функции φ_k мощности k . В связи с этим напомним, что две вершины $\bar{\alpha}_1$ и $\bar{\alpha}_2$ из множества A_f единичных вершин функции $f(x_1, \dots, x_n)$ образуют существенную пару вершин, если не существует подкуба Q такого, что $\bar{\alpha}_1, \bar{\alpha}_2 \in Q$ и $Q \subset A_f$. Совокупность вершин $\bar{\alpha}_1, \dots, \bar{\alpha}_t \in A_f$ образует существенную систему вершин (ССВ), если каждая пара $\bar{\alpha}_i, \bar{\alpha}_j$ — существенная, $i \neq j$, $i, j = 1, \dots, t$ (см. [6, 7, 8]). Если для функции $f(x_1, \dots, x_n)$ найдено представление в виде ДНФ, содержащее t элементарных конъюнкций, а в множестве A_f построена ССВ мощности t , то тем самым доказано, что найденное представление является кратчайшей ДНФ. Для $i = 1, 2$ $\varphi_1 = x_1$, $\varphi_2 = x_1 \bar{x}_2 \vee \bar{x}_1 x_2$ — представление в виде КДНФ.

Пусть $l < k$ и φ_l представлена в виде КДНФ с индексом l , тогда для функции φ_{k-2^s} найдется ССВ мощности $k - 2^s$: $\bar{\alpha}_1, \dots, \bar{\alpha}_{k-2^s}$ и для f_{2^s} существует ССВ мощности 2^s : $\bar{\beta}_1, \dots, \bar{\beta}_{2^s}$, тогда $(1, \bar{\beta}_1), \dots, (1, \bar{\beta}_{2^s}), (0, \bar{\alpha}_1), \dots, (0, \bar{\alpha}_{k-2^s})$ — ССВ мощности k для функции φ_k , и, следовательно, функция φ_k представлена в виде КДНФ. Отсюда имеем $m(k) \leq s + 2$, т. е. $m(k) = s + 1$. Теорема доказана.

Список литературы

1. Никонов В. Г. Конечность некоторых классов булевых функций с ограниченным числом элементарных конъюнкций в ДНФ — Вестник РУДН, 2003. Т. 2, № 1. С. 68–78.

2. Никонов В. Г. О существовании минимальной, но не кратчайшей ортогональной дизъюнктивной нормальной формы — Труды по дискретной математике. Т. 10. — М.: ФИЗМАТЛИТ, 2007. С. 188–201.
3. Журавлев Ю. И. Об алгоритмах упрощения дизъюнктивных нормальных форм — Докл. АН СССР, 1960, т. 132, № 2, с. 260–263.
4. Закревский А. Д. Логический синтез каскадных схем. — М.: Наука, 1981.
5. McGluskey E. J. Minimization of Boolean Functions. — Bell Syst. Techn. J., 1956, v. 35, no 6, pp. 1417–1444.
6. Никонов В. Г. Пороговые представления булевых функций — Обозр. прикл. и промышл. матем., 1994, т. 1, вып. 3, с. 402–457.
7. Никонов В. Г. Классификация минимальных базисных представлений всех булевых функций от четырех переменных — Обозр. прикл. и промышл. матем., 1994, т. 1, вып. 3, с. 458–545.
8. Никонов В. Г. Покрытия булевых графов — Дискрет. матем., 1994, т. 6, вып. 4, с. 21–34.