

## О НИЖНЕЙ ОЦЕНКЕ ФУНКЦИИ ШЕННОНА ДЛИНЫ СЕРТИФИКАТА ПОВТОРНОСТИ БУЛЕВЫХ ФУНКЦИЙ В ОДНОМ СЕМЕЙСТВЕ БАЗИСОВ

### Аннотация.

*Актуальность и цели.* В связи с развитием информатики и цифровой техники актуальным является исследование различных свойств булевых функций. Одним из важных свойств является возможность представления функции в заданном базисе формулой без повторения переменных (бесповторной формулой). Функции, которые можно так представить (бесповторные функции в данном базисе), можно рассматривать как класс «простых» функций в данном базисе. В статье рассматривается следующая задача: для заданной функции требуется найти такой набор строк (сертификат), с помощью которого можно проверить ее повторность в предэлементарном базисе, содержащем функцию семейства дискриминаторных, зависящую от  $s$  переменных. Целью данной работы является улучшение нижней оценки функции Шеннона длины сертификата повторности в этом базисе.

*Материалы и методы.* Используется метод разнозначных матриц и удачный подбор функции с высокой нижней оценкой длины сертификата повторности.

*Результаты и выводы.* Показано, что сертификат повторности функции  $n$  переменных, равной единице только на нулевом и единичном наборах, в этом базисе имеет длину не менее  $n/2 - s + 1$ . Таким образом улучшена известная нижняя оценка  $n/s$  функции Шеннона длины сертификата повторности в этом базисе.

**Ключевые слова:** бесповторная функция, сертификат повторности, семейство дискриминаторных функций, разнозначная матрица.

D. V. Kaftan

## ON THE LOWER BOUND OF THE SHANNON FUNCTION FOR READ-MANY CERTIFICATE LENGTH IN ONE BASE FAMILY

### Abstract.

*Background.* The research of various properties of Boolean functions is an actual problem in connection with the progress of informatics and digital technology. The ability of a function to be represented in a given basis via a formula without replication of variables (a read-once formula) is an important one. The class of functions having this ability may be regarded as a class of “simple” functions in this basis. The author considers a problem of finding a read-many certificate for an arbitrary Boolean function in the extended elementary basis with a discriminator function of  $s$  variables. The object of the article is to improve the lower bound of the Shannon function for read-once certificate length in this basis.

*Materials and methods.* The method named “the matrix of various values” is applied in this paper to a well-selected read-many function with a high lower bound of a read-many certificate.

*Results and conclusion.* The author shows that the length of  $s$  read-many certificate of a function, which equals to 1 only on the sets  $(0, \dots, 0)$  and  $(1, \dots, 1)$ , is not

less than  $n/2 - s + 1$  in this basis. Thus, the researcher has improved the known lower bound  $n/s$  of Shannon function for the certificate length in this basis.

**Key words:** read-once function, read-many certificate, discriminator function, matrix of various values.

Булева функция  $f(x_1, \dots, x_n)$ , представимая (не представимая) формулой без повторения переменных (*бесповторной формулой*) в некотором базисе, называется *бесповторной (повторной)* в этом базисе. Множество  $n$ -мерных булевых наборов  $S$  назовем *сертификатом повторности* функции  $f$  в базисе  $B$ , если для любой бесповторной в базисе  $B$  функции  $h$  существует набор  $x \in S$ , такой что  $f(x) \neq h(x)$ .

Преобразованиями обобщенной однотипности называются замены переменной или самой функции на ее отрицание и перестановка переменных. Функции, получаемые друг из друга конечным числом преобразований обобщенной однотипности, называются обобщенно однотипными.

Длиной сертификата повторности назовем количество наборов в нем.

Функцией Шеннона [1] длины сертификата повторности функций в базисе  $B$  называется наибольшая длина сертификата повторности среди повторных в  $B$  функций  $n$  переменных.

Строку или столбец, состоящие из одних единиц (нулей), будем называть единичными (нулевыми). Обозначим через  $e_i$  строку с одной единицей в  $i$ -й позиции.

Будем называть наследственными базисы, которые содержат все подфункции каждой лежащей в них функции.

Далее рассматриваются только наследственные базисы.

Повторная функция в базисе  $B$  называется слабоповторной, если любая ее подфункция бесповторна в этом базисе. В. А. Стеценко [2] получил все пять семейств слабоповторных функций в элементарном базисе  $B_0 = \{\&, \vee, \neg\}$  с точностью до обобщенной однотипности:

$$f_d^s = x_1(\bar{x}_2 \vee x_3 \cdot \dots \cdot x_s) \vee \bar{x}_2 \cdot \dots \cdot \bar{x}_s, \quad s \geq 3,$$

$$f_t^s = x_1 \cdot \dots \cdot x_s \vee \bar{x}_1 \cdot \dots \cdot \bar{x}_s, \quad s \geq 2,$$

$$f_m^s = x_1(x_2 \vee \dots \vee x_s) \vee x_2 \cdot \dots \cdot x_s, \quad s \geq 3,$$

$$f_4 = x_1(x_2 \vee x_3) \vee x_3 x_4,$$

$$f_5 = x_1(x_3 x_4 \vee x_5) \vee x_2(x_3 \vee x_4 x_5).$$

Семейство  $f_d^s$  называется также семейством дискриминаторных функций.

Рассмотрим семейство базисов  $B_d^s = \{\&, \vee, \neg, f_d^s\}$ . Обозначим через  $T_s(n)$  функцию Шеннона [1] длины сертификата повторности в базисе  $B_d^s$ . В работах [3, 4] исследуется длина сертификата повторности в других базисах. Известно [5], что  $T_s(n) \geq n/s$ . Покажем, что имеет место следующая оценка:

**Теорема.** При  $n > 2s - 4$  верно

$$T_s(n) \geq \frac{n}{2} - s + 3.$$

Известно [5], что функция  $f_t^n$  является повторной в базисе  $B_d^s$  и для доказательства ее повторности в этом базисе достаточно предъявить не более  $n + 2$  наборов – множество  $\{(0, \dots, 0), (1, \dots, 1), e_1, \dots, e_n\}$ .

Докажем, что функцию  $f_t^n$  нельзя отличить от всех бесповторных в  $B_d^s$  функций, равных единице на нулевом и единичном наборах, предъявив менее  $\frac{n}{2} - s + 3$  наборов. Для этого используем метод разнозначных матриц [6]. Назовем 0–1 матрицу разнозначной, если все ее строки различны, и она не имеет ни нулевых, ни единичных строк. Будем говорить, что функция  $f(x_1, \dots, x_n)$  моделирует разнозначную матрицу  $M$  размерности  $k \times n$ , если  $f(0, \dots, 0) = f(1, \dots, 1) = 1$  и  $f(\alpha_1, \dots, \alpha_n) = 0$  для любой строки  $\{\alpha_1, \dots, \alpha_n\}$  матрицы  $M$ .

Будем говорить, что строка имеет 0-преобладание, если в ней количество нулей больше или равно количеству единиц, в противном случае будем говорить, что строка имеет 1-преобладание. В строке с 0-преобладанием (1-преобладанием) значение 0 (соответственно 1) будем называть обычным, а значение 1 (соответственно 0) – особым.

Опишем процедуру разбиения столбцов разнозначной матрицы, которая содержит строки обоих типов.

### Процедура 1

**Дано:** разнозначная матрица  $M$  с  $n > 2s - 4$  столбцами и  $k < \frac{n}{2} - s + 1$

строками, имеющая и строки с 0-преобладанием, и строки с 1-преобладанием. Таким образом, в матрице содержится не менее двух строк. Не ограничивая общности, пусть первая строка матрицы имеет 0-преобладание, а вторая – 1-преобладание. Пусть  $C$  – множество всех столбцов матрицы. Получим из него три множества  $C_1, C_2, C_3$  столбцов, а множество всех строк матрицы разобьем на два множества строк  $R_1, R_2$  согласно следующей процедуре:

(1) Положим  $C_1 = C_2 = C_3 = R_1 = R_2 = \emptyset$ .

(2) До тех пор, пока в  $C_3$  меньше  $s - 2$  столбца и пока не кончились строки, последовательно рассмотрим каждую строку, начиная с первой. Добавим рассматриваемую строку в  $R_1$ . Возможны четыре случая:

(а) Строка имеет 1-преобладание и не имеет нулей на столбцах из  $C_3$ . Тогда у нее есть нуль на каком-то столбце из  $C$ . Переместим этот столбец из  $C$  в  $C_3$ .

(б) Строка имеет 0-преобладание, у нее нет единиц ни на одном столбце из  $C_3$  или  $C_3$  пусто. Тогда в  $C$  есть столбец, на котором она равна единице. Переместим его из  $C$  в  $C_3$ .

(с)  $C_3$  непусто, строка имеет 0-преобладание и у нее есть единица на каком-то столбце из  $C_3$ . Тогда в  $C$  есть столбец, на котором она равна нулю, так как  $(s-2)$  столбца – это меньше половины всех столбцов, а на строке с 0-преобладанием не менее половины столбцов равны нулю. Переместим его из  $C$  в  $C_3$ .

(d) Во всех остальных случаях ничего не делаем.

Таким образом, за  $t$  рассмотренных строк мы добавили не более  $t$  столбцов.

(3) Если закончились строки и  $|C_3| < s-2$ , то переместим еще несколько произвольных столбцов из  $C$  в  $C_3$ , чтобы в  $C_3$  стало  $(s-2)$  столбца.

(4) Обозначим  $x_1, \dots, x_{s-2}$  столбцы из  $C_3$ . Если остались нерассмотренные строки, то для каждой из них сделаем следующее: если у строки есть особенное значение на каком-то столбце из  $C$ , то переместим его из  $C$  в  $C_3$ . Если особые значения у строки есть только на столбцах  $x_1, \dots, x_{s-2}$ , то добавим эту строку в  $R_1$ . Таким образом,  $|C_3| \leq k$ .

(5) Добавим в  $R_2$  все строки матрицы, не вошедшие в  $R_1$ .

(6) Первая рассмотренная в пункте (2) строка имеет 0-преобладание. Тогда она равна единице на каком-то из столбцов  $x_1, \dots, x_{s-2}$  согласно случаю (b) этапа (2). Строка содержит больше половины нулей, а на предыдущих шагах из  $C$  было удалено меньше половины столбцов:

$n - |C_3| \geq n - k > \frac{n}{2}$ , поэтому существует хотя бы один столбец в  $C$ , на котором она равна нулю. Переместим его из  $C$  в  $C_1$ .

(7) Рассмотрим последовательно строки из  $R_1$ , имеющие 1-преобладание. Строка содержит больше половины единиц, а на предыдущих шагах из

$C$  было удалено меньше половины столбцов:  $n - |C_3| - 1 \geq n - k - 1 > \frac{n}{2}$ ,

поэтому остался хотя бы один столбец с единицей либо в  $C_2$ , либо в  $C$ . Если таких столбцов нет в  $C_2$ , то таковой найдется в  $C$ . Переместим его из  $C$  в  $C_2$ .

(8) Рассмотрим последовательно все остальные строки из  $R_1$ , не рассмотренные на этапах (6), (7). Они имеют 0-преобладание. Если у рассматриваемой строки нет нулей ни на каком столбце из  $C_1$ , то либо в  $C$  существует хотя бы один столбец с нулем в этой строке, либо в  $C$  остались только столбцы с единицами в этой строке. Если первое, то переместим столбец с нулем в этой строке из  $C$  в  $C_1$ , если второе – то переместим любой столбец из  $C$  в  $C_2$ .

Заметим, что множества  $C_1$  и  $C_2$  непусты, так как на этапе (6) для первой строки матрицы один столбец добавлен в  $C_1$ , а для второй строки на этапе (7) один столбец добавлен в  $C_2$ . Так как для каждой строки из  $R_1$  было взято не более одного столбца, то  $|C_1| + |C_2| \leq |R_1|$ . Процедура окончена.

Опишем две процедуры разбиения столбцов разнозначной матрицы, все строки которой имеют одинаковое преобладание.

### Процедура 2

**Дано:** разнозначная матрица  $M$  с  $n > 2s - 4$  столбцами и  $k < \frac{n}{2} - s + 1$  строками, имеющими 0-преобладание. Пусть  $C$  – множество всех столбцов матрицы. Получим из него два множества  $C_1, C_2$  столбцов и множество строк  $R_1$  согласно следующей процедуре:

- (1) Положим  $C_1 = C_2 = \emptyset$ .
- (2) Обозначим первые  $(s - 2)$  столбца матрицы  $x_1, \dots, x_{s-2}$ .
- (3) Последовательно для каждой строки, равной нулю на всех этих столбцах, сделаем следующее. Так как матрица разнозначная и  $C_1$  пусто, то либо в  $C_2$ , либо в  $C$  есть столбец с единицей в этой строке. Если такого нет в  $C_2$ , то переместим один такой столбец из  $C$  в  $C_2$ .
- (4) Последовательно для каждой строки, у которой есть единица на каком-то из столбцов  $x_1, \dots, x_{s-2}$ , сделаем следующее. Так как количество строк с нулями во всех этих столбцах не превосходит общего количества строк, то количество выбранных на предыдущем этапе столбцов меньше половины всех столбцов матрицы. Поэтому либо в  $C$ , либо в  $C_1$  у рассматриваемой строки существует столбец, на котором она равна нулю. Если такого нет в  $C_1$ , то переместим один такой столбец из  $C$  в  $C_1$ .
- (5) Если  $C_1$  или  $C_2$  пусто, то добавим туда любой столбец из  $C$ . Это возможно, так как количество выбранных столбцов не превосходит  $k$ , а значит, меньше  $n$ .
- (6) Отметим, что в пунктах (3), (4) мы рассмотрели все строки. Положим  $R_1$  равным множеству всех строк.

Процедура окончена.

### Процедура 3

**Дано:** разнозначная матрица  $M$  с  $n > 2s - 4$  столбцами и  $k < \frac{n}{2} - s + 1$  строками, имеющими 1-преобладание. Пусть  $C$  – множество всех столбцов матрицы. Получим из него два множества  $C_1, C_2$  столбцов и множество строк  $R_1$  согласно следующей процедуре:

- (1) Положим  $C_1 = C_2 = \emptyset$ .
- (2) Обозначим первые  $(s - 2)$  столбца матрицы  $x_1, \dots, x_{s-2}$ .
- (3) Последовательно для каждой строки, равной единице на всех этих столбцах, сделаем следующее. Так как матрица разнозначная и  $C_2$  пусто, то либо в  $C_1$ , либо в  $C$  есть столбец с нулем в этой строке. Если такого нет в  $C_1$ , то переместим один такой столбец из  $C$  в  $C_1$ .
- (4) Последовательно для каждой строки, у которой есть нуль на каком-то из столбцов  $x_1, \dots, x_{s-2}$ , сделаем следующее. Так как количество строк

с единицами во всех этих столбцах не превосходит общего количества строк, то количество выбранных на предыдущем этапе столбцов меньше половины всех столбцов матрицы. Поэтому либо в  $C$ , либо в  $C_2$  у рассматриваемой строки существует столбец, на котором она равна единице. Если такого нет в  $C_2$ , то переместим один такой столбец из  $C$  в  $C_2$ .

(5) Если  $C_1$  или  $C_2$  пусто, то добавим туда любой столбец из  $C$ . Это возможно, так как количество выбранных столбцов не превосходит  $k$ , а значит, меньше  $n$ .

(6) Отметим, что в пунктах (3), (4) мы рассмотрели все строки. Положим  $R_1$  равным множеству всех строк.

Процедура окончена.

Пусть  $x_{i_1}, \dots, x_{i_l}$  – столбцы из  $C_1$ , а  $x_{i_{l+1}}, \dots, x_{i_m}$  – столбцы из  $C_2$ .

Обозначим

$$\begin{aligned} g(x_{i_1}, \dots, x_{i_l}, x_{i_{l+1}}, \dots, x_{i_m}, x_1, \dots, x_{s-2}) = \\ = f_d^s(x_{i_1} \cdot \dots \cdot x_{i_l}, x_{i_{l+1}} \vee \dots \vee x_{i_m}, x_1, \dots, x_{s-2}). \end{aligned}$$

Покажем, какими свойствами обладают множества  $C_1, C_2, R_1$  и функция  $g$  после применения любой из этих процедур:

**Утверждение 1.** Либо  $R_1$  – множество всех строк матрицы, либо  $|R_1| \geq s-2$ .

**Доказательство.** В процедурах 2 и 3 на этапе (6) множество  $R_1$  приравнивается множеству всех строк.

Множество всех строк, рассмотренных на этапе (2) процедуры 1, содержится в  $R_1$ . Если на этом этапе закончились строки, то  $R_1$  – множество всех строк матрицы. Если этот этап закончился при  $|C_3| = s-2$ , то  $|R_1| \geq s-2$ , так как за  $t$  рассмотренных на этом этапе строк мы добавили не более  $t$  столбцов.

**Утверждение 2.** Функция  $g$  равна нулю на множестве  $R_1$ .

**Доказательство.** Если матрица содержит только строки с 0-преобладанием, то для любой строки из  $R_1$  возможны два варианта:

1) она равна нулю на всех столбцах  $x_1, \dots, x_{s-2}$ . Следовательно, на этапе (3) процедуры 2 в  $C_2$  оказался столбец, в котором она равна единице. Следовательно, функция  $g$  равна нулю;

2) она равна единице на каком-то из столбцов  $x_1, \dots, x_{s-2}$ . Тогда на этапе (4) процедуры 2 в  $C_1$  оказался столбец, в котором она равна нулю. Следовательно, функция  $g$  равна нулю.

Если матрица содержит только строки с 1-преобладанием, то для любой строки из  $R_1$  возможны два варианта:

1) она равна единице на всех столбцах  $x_1, \dots, x_{s-2}$ . Тогда на этапе (3) процедуры 3 в  $C_1$  оказался столбец, в котором она равна нулю. Следовательно, функция  $g$  равна нулю;

2) она равна нулю на каком-то из столбцов  $x_1, \dots, x_{s-2}$ . Тогда на этапе (4) процедуры 3 в  $C_2$  оказался столбец, в котором она равна единице. Следовательно, функция  $g$  равна нулю.

Если матрица содержит строки обоих видов, то для любой строки из  $R_1$  возможны три варианта:

1) строка имеет 0-преобладание и равна нулю на каком-то столбце из  $C_1$ . Тогда согласно случаю (b) этапа (2) процедуры 1 и этапу (4) на одной из позиций  $x_1, \dots, x_{s-2}$  есть единица. Следовательно, функция  $g$  равна нулю;

2) строка имеет 0-преобладание и на каждом столбце из  $C_1$  строка равна единице. Согласно случаю (c) этапа (2) процедуры 1 она равна нулю на каком-то столбце из  $x_1, \dots, x_{s-2}$ . На этапе (8) процедуры 1 в  $C_2$  был добавлен столбец с единицей в этой строке. Следовательно, функция  $g$  равна нулю;

3) строка имеет 1-преобладание. Тогда на этапе (7) процедуры 1 в  $C_2$  был добавлен столбец, который равен единице в этой строке. Согласно случаю (a) на этапе (2) и этапу (4), в этой строке на одной из позиций  $x_1, \dots, x_{s-2}$  есть нуль. Следовательно,  $g$  равна нулю на этой строке.

Утверждение доказано.

**Утверждение 3.** Функция  $g$  равна нулю либо на всех строках матрицы, либо не менее чем на  $\frac{|C_1| + |C_2| + s - 2}{2}$  строках.

**Доказательство.** Согласно утверждению 1  $R_1$  либо является множеством всех строк матрицы, либо  $R_1 \geq s - 2$ . В первом случае согласно утверждению 2 функция  $g$  равна нулю на всех строках матрицы.

Пусть  $R_1$  не является множеством всех строк матрицы. Тогда  $|C_1| + |C_2| \leq |R_1|$ , так как на этапах (6), (8) процедуры 1 для каждой строки из  $R_1$  было взято не более одного столбца. Так как  $R_1 \geq s - 2$ , то  $|C_1| + |C_2| + s - 2 \leq |R_1| + s - 2 \leq 2|R_1|$ , следовательно,

$$|R_1| \geq \frac{|C_1| + |C_2| + s - 2}{2}.$$

Утверждение доказано.

**Утверждение 4.** Удаление столбцов из множества  $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$  и строк, на которых  $g$  равна нулю, не приводит к образованию нулевых или единичных строк.

**Доказательство.** Функция  $g$  может быть не равна нулю только на каких-то строках из множества  $R_2$  после применения процедуры 1, так как иначе по утверждению 3 множество  $R_1$  – это множество всех строк матрицы. Рассмотрим любую строку из  $R_2$ . Возможны два варианта:

1) все ее значения на столбцах  $x_1, \dots, x_{s-2}$  обычные. Тогда множества  $C_1$  и  $C_2$  не пересекаются с  $C_3$ , так как каждый столбец перемещался только

один раз из  $C$  в одно из этих множеств. На этапе (4) процедуры 1 в  $C_3$  был добавлен столбец с особым значением в этой строке, поэтому строка имеет особое значение на каком-то столбце из  $C_3$ , отличном от  $x_1, \dots, x_{s-2}$ ;

2) строка имеет особое значение на одном из столбцов  $x_1, \dots, x_{s-2}$ . Тогда строка, так же как в предыдущем случае, имеет особое значение на каком-то столбце из  $C_3$ , отличном от  $x_1, \dots, x_{s-2}$ , иначе оказалась бы в  $R_1$ .

Таким образом, у строки есть столбец с особым значением, не лежащий в  $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$ .

Всего удаляется не более половины столбцов:

$$n - (s - 2) - |C_2| - |C_1| \geq n - s + 2 - k > \frac{n}{2},$$

поэтому существует хотя бы один столбец с обычным значением, не лежащий в  $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$ . Тогда при удалении столбцов  $C_1 \cup C_2 \cup \{x_1, \dots, x_{s-2}\}$  в этой строке останется хотя бы одно особое значение и хотя бы одно обычное, т.е. строка будет разнозначной. Таким образом, удаление из матрицы строк, на которых  $g$  равна нулю, не приводит к образованию нулевых или единичных строк. Утверждение доказано.

Из утверждения 3 следует

**Утверждение 5.** Если  $R_1$  – множество всех строк матрицы, то функция  $g$  ее моделирует.

**Лемма 1.** Для любой разнозначной матрицы  $M$  с  $n > 2s - 4$  столбцами и  $k < \frac{n}{2} - s + 1$  строками всегда найдется неповторная в  $B_d^s$  функция, моделирующая эту матрицу и равная единице на нулевом и единичном наборах.

**Доказательство.** Базис индукции. Пусть  $2s - 4 < n \leq 4s - 8$ . Применив к матрице одну из процедур 1–3, получим множества  $C_1, C_2, R_1$  и функцию  $g$ . Количество строк в матрице меньше  $s - 2$ . Следовательно,  $R_1$  – множество всех строк матрицы, и по утверждению 5 функция  $g$  ее моделирует. Следовательно,  $g$  будет искомой функцией. Заметим, что количество переменных функции  $g$  не превосходит  $2s - 4$ , так как  $|C_1| + |C_2|$  не превосходит  $|R_1|$ .

Индуктивный переход. Пусть  $n > 4s - 8$  и для всех  $n' < n$  (где  $n' > 2s - 4$ ) утверждение леммы выполнено. Применив к матрице одну из процедур 1–3, получим множества  $C_1, C_2, R_1$  и функцию  $g$ . Тогда возможны два варианта:

1)  $R_1$  является множеством всех строк матрицы. Тогда по утверждению 5 функция  $g$  моделирует матрицу  $M$  и является искомой функцией;

2)  $R_1$  не является множеством всех строк матрицы. Получим матрицу  $M'$  из матрицы  $M$  удалением всех строк, на которых  $g$  равна нулю, столбцов из множеств  $C_1, C_2$  и столбцов  $x_1, \dots, x_{s-2}$ . Склеим одинаковые

строки, если таковые имеются. Покажем, что полученная матрица  $M'$  удовлетворяет условиям леммы. Действительно,  $M'$  имеет  $k' = k - |R_1|$  строк и  $n' = n - (|C_1| + |C_2| + s - 2)$  столбцов, для которых выполнено условие

$$\begin{aligned} k' = k - |R_1| &\leq k - \frac{|C_1| + |C_2| + s - 2}{2} < \frac{n}{2} - s + 1 - \frac{|C_1| + |C_2| + s - 2}{2} = \\ &= \frac{n - (|C_1| + |C_2| + s - 2)}{2} - s + 1 < \frac{n'}{2} - s + 1. \end{aligned}$$

Согласно утверждению 4 удаление этих столбцов и строк не приводит к образованию нулевых или единичных строк, поэтому полученная матрица разностная. Следовательно, по предположению индукции, существует неповторная в  $B_d^s$  функция  $g'(y_1, \dots, y_{n'})$ , моделирующая матрицу  $M'$ . Тогда функция  $g \cdot g'$  моделирует матрицу  $M$ . Действительно, на нулевом и единичном наборах обе функции равны единице, а на всех остальных наборах равна нулю либо  $g$  (по утверждению 2), либо  $g'$  (по предположению индукции). Таким образом, функция  $g \cdot g'$  является искомой. Лемма доказана.

**Лемма 2.** Пусть  $n > 2s - 4$  и  $k < \frac{n}{2} - s + 3$ . Тогда для произвольных  $k$  наборов функции  $f_t^n(x_1, \dots, x_n)$  существует неповторная в  $B_d^s$  функция  $g(x_1, \dots, x_n)$ , совпадающая с  $f_t^n$  на этих наборах.

**Доказательство.** Пусть  $A$  – множество из  $k$  наборов функции  $f_t^n(x_1, \dots, x_n)$ . Если среди них нет нулевого или единичного набора, то  $f_t^n$  совпадает на  $A$  с одной из функций  $x_1 \cdot \dots \cdot x_n$  или  $\bar{x}_1 \cdot \dots \cdot \bar{x}_n$ . Если  $A$  содержит и нулевой, и единичный набор, то матрица  $M$ , составленная из остальных наборов  $A$ , является разностной матрицей размера  $(k - 2) \times n$ , где  $k - 2 < \frac{n}{2} - s + 1$ , и удовлетворяет условию леммы 1. Следовательно, существует неповторная в  $B_d^s$  функция  $g(x_1, \dots, x_n)$ , совпадающая с  $f_t^n$  на  $A$ . Лемма доказана.

Из леммы 2 следует утверждение теоремы.

#### Список литературы

1. **Shannon, C. E.** A symbolic analysis of relay and switching circuits / C. E. Shannon // Trans. – 1938. – AIEE 57. – P. 713–723.
2. **Стеценко, В. А.** О предплохих базисах в  $P_2$  / В. А. Стеценко // Математические вопросы кибернетики. – Вып. 4. – М. : Физматлит, 1992. – С. 139–177.
3. **Chistikov, D.** Certificates of Non-Membership for Classes of Read-Once Functions / D. Chistikov, V. Fedorova, A. Voronenko // Fundamenta Informaticae. – 2014. – № 132 (1). – P. 63–77.
4. **Вороненко, А. А.** Повторность булевых функций в элементарном базисе / А. А. Вороненко, В. С. Федорова, Д. В. Чистиков // Известия вузов. Математика. – 2011. – № 11. – С. 72–77.

5. **Вороненко, А. А.** О функции Шеннона для длины сертификата повторности булевых функций в одном семействе базисов / А. А. Вороненко // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. – 2013. – № 4. – С. 45–47.
6. **Вороненко, А. А.** О сложности доказательства повторности булевых функций в бинарном базисе / А. А. Вороненко // Прикладная дискретная математика. – 2011. – № 3 (13). – С. 12–16.

### References

1. Shannon C. E. *Trans.* 1938, AIEE 57, pp. 713–723.
2. Stetsenko V. A. *Matematicheskie voprosy kibernetiki* [Mathematical problems of cybernetics]. Issue 4. Moscow: Fizmatlit, 1992, pp. 139–177.
3. Chistikov D., Fedorova V., Voronenko A. *Fundamenta Informaticae*. 2014, no. 132 (1), pp. 63–77.
4. Voronenko A. A., Fedorova V. S., Chistikov D. V. *Izvestiya vuzov. Matematika* [University proceedings. Mathematics]. 2011, no. 11, pp. 72–77.
5. Voronenko A. A. *Vestnik Moskovskogo universiteta. Ser. 15. Vychislitel'naya matematika i kibernetika* [Bulletin of Moscow University. Series 15. Calculus mathematics and cybernetics]. 2013, no. 4, pp. 45–47.
6. Voronenko A. A. *Prikladnaya diskretnaya matematika* [Applied discrete mathematics]. 2011, no. 3 (13), pp. 12–16.

---

**Кафтан Дарья Владимировна**

аспирант, Московский государственный  
университет имени М. В. Ломоносова  
(Россия, г. Москва, Ленинские горы, 1)

E-mail: blond.programmist@gmail.com

**Kaftan Daria Vladimirovna**

Postgraduate student, Moscow State  
University named after M. V. Lomonosov  
(1 Leninskie gory street, Moscow, Russia)

---

УДК 517.718.7

**Кафтан, Д. В.**

**О нижней оценке функции Шеннона длины сертификата повторности булевых функций в одном семействе базисов / Д. В. Кафтан // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. – 2015. – № 1 (33). – С. 68–77.**