ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 214 (2022). С. 37–43
DOI: 10.36535/0233-6723-2022-214-37-43

УДК 519.714.24

О КЛАССЕ ПОЛИНОМИАЛЬНО УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ

© 2022 г. **О. В. ЗУБКОВ**

Аннотация. Приведены основные свойства полиномиально устойчивых булевых функций. Показано, что любую полиномиально устойчивую функцию можно представить в виде суммы бесповторных в элементарном базисе слагаемых. Рассмотрены связи между полиномиально устойчивыми и симметрическими булевыми функциями. Доказан критерий полиномиальной устойчивости.

Ключевые слова: оператор для булевых функций, полином Жегалкина, бесповторная формула, полиномиальная устойчивость, симметрическая булева функция, вес двоичного набора.

ON THE CLASS OF POLYNOMIALLY STABLE BOOLEAN FUNCTIONS

© 2022 **O. V. ZUBKOV**

Abstract. The basic properties of polynomially stable Boolean functions are examined. We prove that any polynomially stable function can be represented as the sum of terms that are nonrepetitive in an elementary basis. Relationships between polynomially stable and symmetric Boolean functions are discussed and a criterion for polynomial stability is proved.

Keywords and phrases: operator for Boolean functions, Zhegalkin polynomial, repetition-free formula, polynomial stability, symmetric Boolean function, weight of a binary set.

AMS Subject Classification: 93B50

1. Полиномиально устойчивые булевы функции. В работе [1] введен в рассмотрение класс полиномиально устойчивых булевых функций, обладающих рядом интересных свойств. Предварительно определим оператор P на множестве булевых функций одинаковой размерности.

Пусть $f(x_1 \dots, x_n)$ — булева функция, заданная своим вектором длины 2^n. Построим для нее полином Жегалкина и натуральным образом упорядочим его коэффициенты. Получим двоичный вектор h длины 2^n, в котором h_i соответствует наличию или отсутствию слагаемого, для которого двоичное представление i является маской по включению. Если вектор коэффициентов полинома Жегалкина был получен методом треугольника, то вектор h находится на его диагонали. Таким образом, вектору f естественным образом ставится в соответствие вектор (и булева функция) h. Обозначим $h = P(f)$.

В [1] доказаны следующие свойства оператора P:

1. $P(f \oplus g) = P(f) \oplus P(g)$.
2. Если $x_{i_1}, \dots x_{i_n}$ — произвольная перестановка переменных, то

$$P(f(x_{i_1}, \dots, x_{i_n})) = P(f)(x_{i_1}, \dots, x_{i_n}).$$

Далее под $f^0_{x_i}$ и $f^1_{x_i}$ будем понимать соответственно нулевую и единичную остаточную по аргументу x_i функции f.

3. $P(f) = \overline{x}_i P(f^0_{x_i}) \oplus x_i(P(f^0_{x_i} \oplus f^1_{x_i}))$ для любой x_i.

   Далее для наглядности будем при переходе к остаточным вместо $f = \overline{x}_i f^0_{x_i} \oplus x_i f^1_{x_i}$ записывать

$$f = \begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix}.$$

Тогда данное свойство будет иметь вид

$$P(f) = \begin{pmatrix} P(f^0_{x_i}) \\ P(f^0_{x_i} \oplus f^1_{x_i}) \end{pmatrix}. \tag{1}$$

4. Оператор P является инволютивным, то есть $P(P(f)) = f$.

Определение 1. Будем говорить, что булева функция f является полиномиально устойчивой, если $P(f) = f$.

5. Для любой булевой функции f верно, что $f \oplus P(f)$ полиномиально устойчива.

Определение 2. Будем говорить, что f принадлежит классу полиномиально устойчивой функции $f \oplus P(f)$. Для этой функции введем обозначение: $c(f) = f \oplus P(f)$.

6. $P(f) = f \oplus c(f)$, $c(f \oplus g) = c(f) \oplus c(g)$. Если f — полиномиально устойчивая, то $c(f) = 0$ и любая перестановка переменных у полиномиально устойчивой функции оставляет ее полиномиально устойчивой.
7. Если

$$f = \begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix}$$

   является полиномиально устойчивой, то верно, что $f^0_{x_i}$ — полиномиально устойчивая и $f^1_{x_i}$ принадлежит классу $f^0_{x_i}$. Действительно, так как $f = P(f)$, то

$$\begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix} = \begin{pmatrix} P(f^0_{x_i}) \\ P(f^0_{x_i} \oplus f^1_{x_i}) \end{pmatrix}.$$

   Значит, $f^0_{x_i} = P(f^0_{x_i})$ и $f^0_{x_i}$ полиномиально устойчивая. Далее,

$$f^1_{x_i} = P(f^0_{x_i} \oplus f^1_{x_i}) = P(f^0_{x_i}) \oplus P(f^1_{x_i}),$$

   то есть

$$f^0_{x_i} = f^1_{x_i} \oplus P(f^1_{x_i}).$$

   Последнее равенство говорит, что $f^1_{x_i}$ принадлежит классу $f^0_{x_i}$.
8. Пусть f и $c(f)$ зависят от $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_n$. Тогда функция $\overline{x}_i c(f) \oplus x_i f$ является полиномиально устойчивой, причем в ее класс входит функция $\overline{x}_i f \oplus x_i f$ с фиктивным аргументом x_i.

   Для этого заметим следующее:

$$P\begin{pmatrix} c(f) \\ f \end{pmatrix} = \begin{pmatrix} P(c(f)) \\ P(c(f) \oplus f) \end{pmatrix} = \begin{pmatrix} c(f) \\ c(f) \oplus P(f) \end{pmatrix} = \begin{pmatrix} c(f) \\ f \end{pmatrix},$$

$$\begin{pmatrix} f \\ f \end{pmatrix} \oplus P\begin{pmatrix} f \\ f \end{pmatrix} = \begin{pmatrix} f \\ f \end{pmatrix} \oplus \begin{pmatrix} P(f) \\ P(0) \end{pmatrix} = \begin{pmatrix} f \oplus P(f) \\ f \end{pmatrix} = \begin{pmatrix} c(f) \\ f \end{pmatrix}.$$

9. Множество полиномиально устойчивых функций от n аргументов образует абелеву группу по операции $\oplus$, которую обозначим G_n.

   Если $f \in G_n$ и $g \in G_n$, то $P(f \oplus g) = P(f) \oplus P(g) = f \oplus g$, то есть G_n замкнута по операции $\oplus$.

   $P(0) = 0$, то есть нейтральный по $\oplus$ элемент $\in G_n$.

   Для любой $f \in G_n$ она является сама к себе обратной по $\oplus$.
10. Пусть f — полиномиально устойчивая от n аргументов и множество булевых функций $K(f)$ — класс ее функций, то есть из того, что $g \in K(f)$, следует, что $c(g) = f$. Тогда $K(f)$ является классом смежности по подгруппе G_n.

Действительно, пусть f' — произвольная полиномиально устойчивая функция из G_n и $g \in K(f)$. Согласно пункту 8, хотя бы одна такая функция, равная

$$\begin{pmatrix} f^1_{x_i} \\ f^1_{x_i} \end{pmatrix},$$

существует. Рассмотрим, какому классу принадлежит $g \oplus f'$:

$$c(g \oplus f') = c(g) \oplus c(f') = c(g) \oplus 0 = c(g) = f,$$

то есть $g \oplus f' \in K(f)$. Обратно, пусть $g' \in K(f)$; покажем, что существует такая $f' \in G_n$, что $g' = g \oplus f'$. Очевидно, что $f' = g \oplus g'$; покажем, что f' полиномиально устойчива:

$$P(f') = P(g \oplus g') = P(g) \oplus P(g') = g \oplus c(g) \oplus g' \oplus c(g') = g \oplus f \oplus g' \oplus f = g \oplus g' = f'.$$

Пусть $f \otimes g$ — кронекерово произведение функции f на функцию g (в векторе f заменим все единицы на вектор g, а все нули — на вектор из нулей такой же длины, как и вектор g).

11. Верно, что $P(f \otimes g) = P(f) \otimes P(g)$. Покажем это при помощи матиндукции по числу аргументов функции f. $P(0 \otimes g) = P(0) \otimes P(g)$ — получится вектор из нулей, длина которого равна длине вектора g. $P(1 \otimes g) = P(1) \otimes P(g) = P(g)$:

$$P(f \otimes g) = P\begin{pmatrix} f^0_{x_1} \otimes g \\ f^1_{x_1} \otimes g \end{pmatrix} = \begin{pmatrix} P(f^0_{x_1} \otimes g) \\ P((f^0_{x_1} \otimes g) \oplus (f^1_{x_1} \otimes g)) \end{pmatrix} = \begin{pmatrix} P(f^0_{x_1} \otimes g) \\ P((f^0_{x_1} \oplus f^1_{x_1}) \otimes g) \end{pmatrix} =$$
$$= \begin{pmatrix} P(f^0_{x_1}) \otimes P(g) \\ P(f^0_{x_1} \oplus f^1_{x_1}) \otimes P(g)) \end{pmatrix} = \begin{pmatrix} P(f^0_{x_1}) \\ P((f^0_{x_1} \oplus f^1_{x_1})) \end{pmatrix} \otimes P(g) = P(f) \otimes P(g).$$

12. Если f и g полиномиально устойчивы, то $f \otimes g$ также полиномиально устойчива. Действительно, $P(f \otimes g) = P(f) \otimes P(g) = f \otimes g$.

2. Представление полиномиально устойчивых функций суммами бесповторных в элементарном базисе слагаемых. В [2] показано, что свойство 12 и тот факт, что функции конъюнкция и дизъюнкция являются полиномиально устойчивыми, логически влекут, что бесповторная конъюнкция двух полиномиально устойчивых функций $f(x_1, \ldots, x_k)\&g(x_{k+1}, \ldots, x_n)$ является полиномиально устойчивой. Из этого вытекает следующее утверждение.

Утверждение 1. *Пусть множество $X = \{x_1, \ldots, x_n\}$ разбито на подмножества $X_1, X_2, \ldots, X_m$ так, что $X_i \cap X_j = \varnothing$ при $i \neq j$ и $X_1 \cup \ldots \cup X_m = X$. Тогда бесповторная конъюнкция дизъюнкций переменных каждого класса разбиения вида*

$$\left(\bigvee_{x_i \in X_1} x_i\right) \cdot \left(\bigvee_{x_i \in X_2} x_i\right) \cdot \ldots \cdot \left(\bigvee_{x_i \in X_m} x_i\right) \tag{2}$$

является полиномиально устойчивой.

Пример 1. Пусть $n = 6$ и $X = \{x_1, x_4\} \cup \{x_2, x_5, x_6\} \cup \{x_3\}$. Непосредственной проверкой можно убедиться, что функция $(x_1 \vee x_4) \cdot (x_2 \vee x_5 \vee x_6) \cdot x_3$ является полиномиально устойчивой.

Множество функций, представимых в виде бесповторных формул вида (2) образует базисное множество для полиномиально устойчивых функций. Это вытекает следует из следующего утверждения.

Утверждение 2. *Любую полиномиально устойчивую функцию, за исключением тождественного нуля, можно представить (возможно, несколькими способами) в виде суммы бесповторных конъюнкций вида* (2).

Доказательство. Покажем, как можно найти указанное представление для произвольной полиномиально устойчивой функции f. Разложим f по двум переменным:

$$f = \begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix} = \begin{pmatrix} f^{0\,0}_{x_i x_j} \\ f^{0\,1}_{x_i x_j} \\ f^{1\,0}_{x_i x_j} \\ f^{1\,1}_{x_i x_j} \end{pmatrix} = \begin{pmatrix} c(f^{0\,1}_{x_i x_j}) \\ f^{0\,1}_{x_i x_j} \\ f^{1\,0}_{x_i x_j} \\ f^{1\,1}_{x_i x_j} \end{pmatrix} = \begin{pmatrix} c(g_1) \\ g_1 \\ g_2 \\ g_3 \end{pmatrix},$$

где $g_1 = f^{0\,1}_{x_i x_j}$. Рассмотрим функцию

$$g = \begin{pmatrix} c(g_1) \\ g_1 \\ g_1 \\ g_1 \end{pmatrix}.$$

Так как

$$c\begin{pmatrix} g_1 \\ g_1 \end{pmatrix} = \begin{pmatrix} c(g_1) \\ g_1 \end{pmatrix},$$

то функция g является полиномиально устойчивой. Полиномиально устойчивая функция

$$\begin{pmatrix} c(g_1) \\ g_1 \end{pmatrix} = f^0_{x_i}$$

зависит от переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$. Подставим в эту функцию вместо переменной x_j выражение $x_i \vee x_j$ и получим формулу

$$\Phi = f^0_{x_i}\big(x_1,\ \ldots,\ x_{i-1},\ x_{i+1},\ \ldots,\ x_{j-1},\ x_i \vee x_j,\ x_{j+1}, \ldots,\ x_n\big).$$

Покажем, что эта формула реализует функцию g. Действительно,

$$\Phi^{0\,0}_{x_i x_j} = f^{0\,0}_{x_i x_j} = c(g_1), \quad \Phi^{0\,1}_{x_i x_j} = \Phi^{1\,0}_{x_i x_j} = \Phi^{1\,1}_{x_i x_j} = f^{0\,1}_{x_i x_j} = g_1.$$

Далее рассмотрим функцию $h = f \oplus g$. Так как h является суммой двух полиномиально устойчивых функций, то и сама она полиномиально устойчива. Очевидно, что $h^0_{x_i} = 0$,

$$h^1_{x_i} = \begin{pmatrix} g_2 \oplus g_1 \\ g_3 \oplus g_1 \end{pmatrix},$$

и так как $c\big(h^1_{x_1}\big) = 0$, то и сама $h^1_{x_i}$ тоже полиномиально устойчивая. При этом $h = x_i \cdot h^1_{x_i}$. В итоге получаем, что любую полиномиально устойчивую булеву функцию $f = g \oplus h$ можно представить в виде формулы над двумя полиномиально устойчивыми функциями меньшей размерности $f^0_{x_i}$ и $h^1_{x_i}$:

$$f = f^{0(x_i \vee x_j)}_{x_i x_j} \oplus x_i \cdot h^1_{x_i}. \tag{3}$$

Далее воспользуемся математической индукцией по числу аргументов функции f. Если в разложении (3) оба остаточных члена являются унарными, то первое слагаемое превращается в дизъюнкцию, а второе в конъюнкцию двух переменных. Оба эти слагаемых имеют вид (2). Если $f^0_{x_i}$ и $h^1_{x_i}$ не унарные, то каждую из них представим в виде суммы слагаемых вида (2) и подставим это представление в (3) для основной функции f. В левой части полученной формулы вместо одной из переменных появится дизъюнкция двух переменных, в правой части формулы каждое слагаемое умножится на x_i. И в том и в другом случае каждое слагаемое полученной формулы сохранит вид (2). □

3. Критерий полиномиальной устойчивости булевых функций.

Теорема 1. *Булева функция $f(x_1, \ldots, x_n)$ является полиномиально устойчивой тогда и только тогда, когда любая её нулевая остаточная является полиномиально устойчивой, и количество единиц в векторе f на всех наборах, кроме последнего, четно.*

Доказательство. Докажем, что значение последнего бита функции $P(f)$ равно сумме по mod2 всех битов исходной функции f. Для этого поочередно разложим её по каждой переменной при помощи формулы (1):

$$P(f) = \begin{pmatrix} P(f^0_{x_1}) \\ P(f^0_{x_1}) \oplus P(f^1_{x_1}) \end{pmatrix} = \begin{pmatrix} P(f^{0\,0}_{x_1 x_2}) \\ P(f^{0\,0}_{x_1 x_2}) \oplus P(f^{0\,1}_{x_1 x_2}) \\ P(f^{0\,0}_{x_1 x_2}) \oplus P(f^{1\,0}_{x_1 x_2}) \\ P(f^{0\,0}_{x_1 x_2}) \oplus P(f^{1\,0}_{x_1 x_2}) \oplus P(f^{0\,1}_{x_1 x_2}) \oplus P(f^{1\,1}_{x_1 x_2}) \end{pmatrix}.$$

Проведя это разложение по всем переменным, на последней позиции в функции $P(f)$ получим

$$\bigoplus_{(\sigma_1,\ldots,\sigma_n)} P(f(\sigma_1,\ldots,\sigma_n)).$$

Так как для нульместных функций $P(0)=0$ и $P(1)=1$, то получим, что

$$P(f)(1,\ldots,1)=\bigoplus_{(\sigma_1,\ldots,\sigma_n)} f(\sigma_1,\ldots,\sigma_n),$$

что и требовалось доказать. Теперь перейдем к доказательству основного утверждения теоремы. Пусть f — полиномиально устойчива. Тогда все её нулевые остаточные так же полиномиально устойчивы. Далее, так как $P(f)=f$, то из вышедоказанного свойства получим, что

$$f(1,\ldots,1)=P(f)(1,\ldots,1)=\bigoplus_{(\sigma_1,\ldots,\sigma_n)} f(\sigma_1,\ldots,\sigma_n).$$

Отсюда получаем, что

$$\bigoplus_{(\sigma_1,\ldots,\sigma_n)\neq(1,\ldots,1)} f(\sigma_1,\ldots,\sigma_n)=0,$$

что и требовалось. Обратно, пусть все нулевые остаточные функции f являются полиномиально устойчивыми и

$$\bigoplus_{(\sigma_1,\ldots,\sigma_n)\neq(1,\ldots,1)} f(\sigma_1,\ldots,\sigma_n)=0.$$

Покажем, что тогда $P(f)=f$.

Для любого набора $(\sigma_1,\ldots,\sigma_n)\neq(1,\ldots,1)$ найдется по крайней мере одна нулевая остаточная, в которую этот набор входит, а значит, $P(f)(\sigma_1,\ldots,\sigma_n)=f(\sigma_1,\ldots,\sigma_n)$, так как эта нулевая остаточная полиномиально устойчива. Но равенство

$$\bigoplus_{(\sigma_1,\ldots,\sigma_n)\neq(1,\ldots,1)} f(\sigma_1,\ldots,\sigma_n)=0$$

эквивалентно равенству

$$\bigoplus_{(\sigma_1,\ldots,\sigma_n)} f(\sigma_1,\ldots,\sigma_n)=f(1,\ldots,1),$$

а значит, по вышедоказанному свойству, $f(1,\ldots,1)=P(f)(1,\ldots,1)$, то есть функции $P(f)$ и f совпадают на всех наборах. □

Пример 2. Рассмотрим полиномиально устойчивую булеву функцию

$$f=(0110\ 1101\ 1100\ 1001).$$

Её нулевые остаточные (0110 1101), (0110 1100), (0111 1110) и (0110 1010) являются полиномиально устойчивыми. Количество единиц в векторе f на всех позициях, кроме последней, равно 8, то есть четно.

4. Симметрические полиномиально устойчивые булевы функции. Выше уже было показано, что любая полная бесповторная конъюнкция элементарных дизъюнкций вида

$$\bigwedge(x_{i_1}\vee x_{i_2}\vee\ldots\vee x_{i_k})$$

является полиномиально устойчивой. Далее было показано, что любую полиномиально устойчивую функцию можно представить (возможно, несколькими способами) в виде суммы таких бесповторных конъюнкций. Таким образом, достаточно интересным является вопрос минимизации представления произвольной полиномиально усточивой функции в классе таких сумм. При рассмотрении вопросов минимизации было замечено, что большую роль здесь могут играть симметрические полиномиально устойчивые булевы функции. Например, для случая четырех переменных, кроме полной дизъюнкции $x_1\vee x_2\vee x_3\vee x_4$, все остальные бесповторные конъюнкции

естественным образом разбиваются на классы, такие, что сумма внутри каждого класса равна одной и той же симметрической функции:

$$x1(x_2 \vee x_3 \vee x_4) \oplus x_2(x_1 \vee x_3 \vee x_4) \oplus x_3(x_1 \vee x_2 \vee x_4) \oplus x_4(x_1 \vee x_2 \vee x_3) = (0000\ 0001\ 0001\ 0110),$$
$$(x_1 \vee x_2)x_3x_4 \oplus x_1x_2(x_3 \vee x_4) = (0000\ 0001\ 0001\ 0110),$$
$$(x_1 \vee x_3)x_2x_4 \oplus x_1x_3(x_2 \vee x_4) = (0000\ 0001\ 0001\ 0110),$$
$$(x_1 \vee x_4)x_2x_3 \oplus x_1x_4(x_2 \vee x_3) = (0000\ 0001\ 0001\ 0110),$$
$$(x_1 \vee x_2)(x_3 \vee x_4) \oplus (x_1 \vee x_3)(x_2 \vee x_4) \oplus (x_1 \vee x_4)(x_2 \vee x_3) \oplus x_1x_2x_3x_4 = (0000\ 0001\ 0001\ 0110).$$

В связи с этим содержательным является вопрос о количестве симметрических полиномиально устойчивых функций, и их виде. Для начала полезно рассмотреть симметрические функции элементарного вида, такие, что они на всех наборах равны 0, за исключением наборов одного фиксированного веса w, на которых они равны 1. Например, упомянутая выше функция (0000 0001 0001 0110) равна 0 везде, кроме наборов веса 3. Обозначим функцию от n аргументов, такую, что она равна 1 только на наборах веса w через $f(n, w)$. Очевидно, что при $n < w$ эта функция равна тождественно нулевой, а при $n = w$ она будет равна 1 только на последнем наборе. То есть при $n \leqslant w$ функция $f(n, w)$ всегда полиномиально устойчива. Содержательный интерес вызывает следующий вопрос: при каких условиях $f(n, w)$ является полиномиально устойчивой для $n > w$? При этом следует учитывать, что если в какой-то момент $f(n, w)$ не является полиномиально устойчивой, то и для любого $k > n$ $f(k, w)$ так же не является полиномиально устойчивой, так как любая нулевая остаточная у полиномиально устойчивой функции так же должна быть полиномиально устойчивой, а $f(n, w)$ является нулевой остаточной у $f(n + 1, w)$ и так далее. Рассмотрим первые значения n и w: $f(1, 1) = (01)$ — полиномиально устойчива, $f(2, 1) = (0110)$ — полиномиально устойчива, $f(3, 1) = (0110\ 1000)$ — не полиномиально устойчива. $f(2, 2) = (0001)$ — полиномиально устойчива, $f(3, 2) = (0001\ 0110)$ — не полиномиально устойчива. $f(3, 3) = (0000\ 0001)$ — полиномиально устойчива, $f(4, 3) = (0000\ 0001\ 0001\ 0110)$ — полиномиально устойчива, $f(5, 3) = (0000\ 0001\ 0001\ 0110\ 0001\ 0110\ 0110\ 1000)$ — полиномиально устойчива, $f(6, 3) = (0000\ 0001\ 0001\ 0110\ 0001\ 0110\ 0110\ 1000\ 0001\ 0110\ 0110\ 1000\ 0110\ 1000\ 1000\ 0000)$ — полиномиально устойчива, $f(7, 3)$ полиномиально устойчивой не является. Видно, что вопрос не является тривиальным. Общее описание полиномиально устойчивых булевых функций указанного вида дано в следующей теореме:

Теорема 2. *Пусть число $w+1$ делится на 2^k и не делится на 2^{k+1}. Тогда все функции $f(i, w)$ для i от 0 до $w + 2^k - 1$ включительно будут полиномиально устойчивыми, а $f(w + 2^k, w)$ и все последующие будут не полиномиально устойчивыми.*

Доказательство. Рассмотрим бесконечную последовательность весов двоичных наборов при их натуральном упорядочении:

$$0\ 1\ 1\ 2\ 1\ 2\ 2\ 3\ 1\ 2\ 2\ 3\ 2\ 3\ 3\ 4\ldots$$

Эта последовательность в энциклопедии целочисленных последовательностей OEIS (см. [3] и онлайн-версию) имеет номер A000120. Данная последовательность строится следующим образом: на нулевом шаге берем 0 и далее на каждом последующем шаге последовательность получается из предыдущей путем приписывания в её конец этой же последовательности с увеличением каждого её элемента на 1. Если взять префикс этой последовательности длины 2^n и заменить в ней все числа, равные w на 1, а остальные на 0, то получим $f(n, w)$. Пусть для $(n - 1)$-го шага построения этой последовательности среди первых 2^{n-1} её элементов имеется $D(n - 1, w)$ чисел w. Тогда на n-м шаге среди первых 2^n элементов будет $D(n - 1, w) + D(n - 1, w - 1)$ чисел w, так как в добавленной второй половине каждое число из первой половины увеличено на 1. В совокупности с условиями $D(w, 0) = 1$ и $D(w, w) = 1$, получаем, что $D(n, w)$ равно обычному биномиальному коэффициенту $\binom{n}{w}$. Таким образом, для фиксированного w, в функции $f(n, w)$ будет $\binom{n}{w}$ единиц. Исходя из критерия, доказанного в теореме 1, нас будет итересовать четность количества чисел w среди первых $2^n - 1$ элементов последовательности A000120. То есть нас будет

интересовать треугольник Паскаля по модулю 2, называемый также треугольником Серпинского. В этом треугольнике будем выделять строки, столбцы и диагонали. За счет симметричности треугольника Паскаля, соответствующие столбцы и диагонали совпадают. Найдем первое $n > w$, такое, что $\binom{n}{w}$ нечетно. Для этого в треугольнике Серпинского рассмотрим столбец с номером w (нумерация столбцов с 0), и в этом столбце найдем первую единицу, стоящую не на верхней диагонали треугольника. Пусть строка треугольника Серпинского, в которой находится эта первая встреченная единица, имеет номер T (нумерация строк с 0), $T > w$. Покажем, что все $f(i, w)$ для i от 0 до $T - 1$ являются полиномиально устойчивыми, а $f(T, w)$ — не полиномиально устойчивая. Действительно, мы уже зафиксировали, что $f(w, w)$ — полиномиально устойчива. Так как для любой $f(n, w)$ все её нулевые остаточные в силу симметричности равны $f(n - 1, w)$, то для того, чтобы $f(n, w)$ была полиномиально устойчивой, требуется согласно критерию теоремы 1 полиномиальная устойчивость предыдущей $f(n-1, w)$ и четность биномиального коэффициента $\binom{n}{w}$. Если он четен, то и $f(n, w)$ будет полиномиально устойчива, если он нечетен, то и $f(n, w)$ и все последующие $f(n + i, w)$ не будут полиномиально устойчивыми, то есть все $f(i, w)$ для i от 0 до $T - 1$ являются полиномиально устойчивыми, а $f(T, w)$ и все последующие — не полиномиально устойчивы. Итак, пусть $2^{n-1} \leqslant w < 2^n - 1$. В силу самоподобия треугольника Серпинского, а также того, что его строки с номерами $2^i - 1$ полностью заполнены единицами, можно заметить, что треугольная область, состоящая из столбцов с номерами $2^{n-1}, 2^{n-1} + 1, \ldots, 2^n - 1$, ограниченных снизу $(2^n - 1)$-й строкой, совпадает с треугольной областью, состоящей из столбцов $0, 1, \ldots, 2^{n-1} - 1$, ограниченных снизу $(2^{n-1} - 1)$-й строкой. Если $w = 2^{n-1} - 1$, то в этом столбце первая единица встретится в строке номер $2^n - 1$, то есть $T = 2^n - 1 = w + 2^{n-1}$ — это первое значение, на котором $f(T, w)$ будет не полиномиально устойчивой. Так как в этом случае $w + 1$ делится на 2^{n-1} и не делится на 2^n, то утверждение теоремы верно. Иначе, если $w > 2^{n-1} - 1$, то перейдем от рассмотрения этого столбца к рассмотрению равного ему в пределах рассматриваемых треугольных областей столбца $w - 2^{n-1}$ и повторим предыдущее рассуждение. В результате вычитания некоторого количества старших степеней двойки число w преобразуется к виду $2^k - 1$, что означает, что первая единица в столбце номер w встретится на строке номер $w + 2^k - 1$. Так как $w + 1$ в этом случае делится на 2^k, но не делится на 2^{k+1}, то теорема доказана. □

СПИСОК ЛИТЕРАТУРЫ

1. *Зубков О. В.* О классе полиномиально устойчивых булевых функций и их свойствах// Мат. 5 Российской школы-семинара «Синтаксис и семантика логических систем» (8–12 августа 2017, Улан-Удэ). — Улан-Удэ: Изд-во БГУ, 2017. — С. 87–91.
2. *Зубков О. В.* Представление полиномиально устойчивых функций суммами бесповторных в элементарном базисе слагаемых// Мат. 6 Междунар. школы-семинара «Синтаксис и семантика логических систем» (11–16 августа 2019, Ханх, Монголия). — Иркутск: Изд-во ИГУ, 2019. — С. 48–52.
3. *Sloane N. J. A., Plouffe S.* The encyclopedia of integer sequences. — San Diego: Academic Press, 1995.

Зубков Олег Владимирович
Иркутский государственный университет
E-mail: oleg.zubkov@mail.ru