Д.С. Романов

О ТЕСТАХ ОТНОСИТЕЛЬНО ПЕРЕСТАНОВОК ПЕРЕМЕННЫХ В БУЛЕВЫХ ФУНКЦИЯХ *

Вводные определения

В статье изучается поведение функций Шеннона длины диагностического и проверяющего теста относительно произвольных перестановок переменных, а также относительно произвольных перестановок и отрицаний переменных в булевой функции, зависящей от n переменных.

Пусть $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ – набор значений булевых переменных $x_1, x_2, \ldots, x_n$ ($n \in \mathbb{N}$). Множество всех таких наборов $\tilde{\alpha}$ образует *n-мерный булев куб*, обозначаемый через E_2^n. *Весом* набора $\tilde{\alpha}$ называется число единиц в наборе $\tilde{\alpha}$ (обозначение: $\|\tilde{\alpha}\|$). Множество всех наборов из E_2^n, имеющих вес k, называется *k-м слоем булева куба* E_2^n и здесь обозначается через $E_2^n(k)$. Через $\rho(\tilde{\alpha}', \tilde{\alpha}'')$ ($\tilde{\alpha}', \tilde{\alpha}'' \in E_2^n$) будем обозначать *расстояние Хемминга* между наборами (вес покоординатной суммы наборов $\tilde{\alpha}'$ и $\tilde{\alpha}''$ по модулю 2).

Пусть $f(\tilde{x}^n)$ – булева функция, формально зависящая от переменных $x_1, x_2, \ldots, x_n$. Обозначим $N_f = \{\tilde{\alpha} \mid \tilde{\alpha} \in E_2^n, f(\tilde{\alpha}) = 1\}$.

Пусть, далее, Γ – некоторая группа (относительно композиции) биекций на множестве E_2^n. При этом, если $\zeta \in \Gamma$ ($\zeta = \zeta(\tilde{x}^n) : E_2^n \to E_2^n$ – взаимно однозначное отображение на множестве E_2^n), то ζ^{-1} – биекция, обратная к ζ. (Ясно, что в группе Γ содержится тождественное отображение $e : E_2^n \to E_2^n$, являющееся единицей группы). Обозначим через $f_\zeta(\tilde{x}^n)$ функцию, полученную из функции $f(\tilde{x}^n)$ действием отображения ζ (т. е. $f_\zeta(\tilde{x}^n) = f(\zeta(\tilde{x}^n))$, или, что то же самое, для любого $\tilde{\alpha} \in E_2^n$ $f_\zeta(\tilde{\alpha}) = f(\zeta(\tilde{\alpha}))$). Через $\Gamma(f)$ обозначим множество всех булевых функций, полученных из f действием отображений $\zeta \in \Gamma$: $\Gamma(f) = \{f_\zeta \mid \zeta \in \Gamma\}$. Очевидно, что $f = f_e \in \Gamma(f)$.

Введем два важных частных случая для Γ. Обозначим через $\mathfrak{L}$

(соответственно, через $\mathfrak{S}$) группу Γ всех биекций на множестве E_2^n, индуцированных всевозможными перестановками и отрицаниями переменных x_1, x_2, $\dot{s}$, x_n (соответственно, группу Γ всех биекций на множестве E_2^n, индуцированных всевозможными перестановками переменных x_1, x_2, …, x_n). Более формально, пусть $\phi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ – подстановка на множестве $\{1,2,\dots,n\}$ (лежащая в симметрической группе S_n), а $\tilde{\varepsilon} = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ – набор из E_2^n. Для каждого набора $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in E_2^n$ определим

$$\zeta_\phi(\tilde{\alpha}) = (\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n}),$$

$$\zeta_{\tilde{\varepsilon}}(\tilde{\alpha}) = \tilde{\alpha} \oplus \tilde{\varepsilon} = (\alpha_1 \oplus \varepsilon_1, \alpha_2 \oplus \varepsilon_2, \dots, \alpha_n \oplus \varepsilon_n).$$

Так определяются биекции ζ_ϕ и $\zeta_{\tilde{\varepsilon}}$. Группа $\mathfrak{L}$ порождена множеством биекций $\{\zeta_\phi(\zeta_{\tilde{\varepsilon}}) \mid \phi \in S_n, \tilde{\varepsilon} \in E_2^n\}$, а группа $\mathfrak{S}$ – множеством биекций $\{\zeta_\phi \mid \phi \in S_n\}$.

Множество T наборов значений переменных $x_1, x_2, \dots, x_n$ называется *диагностическим* (соответственно, *проверяющим*) *тестом относительно действия группы* Γ *над булевой функцией* $f(x_1, x_2, \dots, x_n)$ тогда и только тогда, когда любые две не равные друг другу функции $f_{\zeta_1}(\tilde{x}^n)$ и $f_{\zeta_2}(\tilde{x}^n)$ из $\Gamma(f)$ различаются на множестве T (соответственно, когда любая не равная f функция $f_\zeta(\tilde{x}^n)$ из $\Gamma(f)$ отличается от f на множестве T). Число наборов в тесте T называется его *длиной* и обозначается $|T|$ или $l(T)$. Тест минимальной длины называется *минимальным*. Длину минимального диагностического теста относительно действия группы Γ над булевой функцией $f(\tilde{x}^n)$ будем обозначать через $l_\Gamma^{diagn}(f(\tilde{x}^n))$, а длину минимального проверяющего теста относительно действия группы Γ над булевой функцией $f(\tilde{x}^n)$ – через $l_\Gamma^{detect}(f(\tilde{x}^n))$. Введем функции Шеннона длины диагностического и проверяющего теста относительно действия группы Γ над булевой функцией:

$$l_\Gamma^{diagn}(n) = \max_{f(\tilde{x}^n) \in P_2^n} l_\Gamma^{diagn}(f(\tilde{x}^n)),$$

$$l_\Gamma^{detect}(n) = \max_{f(\tilde{x}^n) \in P_2^n} l_\Gamma^{detect}(f(\tilde{x}^n)).$$

Отметим, что тест относительно действия группы $\mathfrak{S}$ над булевой функцией $f(\tilde{x}^n)$ называется *тестом относительно произвольных перестановок переменных булевой функции* $f(\tilde{x}^n)$, а тест относительно действия группы $\mathfrak{L}$ над булевой функцией $f(\tilde{x}^n)$ – *тестом*

относительно произвольных перестановок и отрицаний переменных булевой функции $f(\tilde{x}^n)$.

О функции Шеннона длины диагностического теста относительно перестановок переменных

В этом разделе на основании анализа конкретных булевых функций будут получены асимптотические оценки вида 2^n функций Шеннона длины диагностического теста относительно произвольных перестановок, а также перестановок и отрицаний переменных.

Рассмотрим булеву функцию

$$h(\tilde{x}^n) = \overline{x}_1 x_2 \,\&\ldots\&\, x_{n-1}x_n \vee \overline{x}_1\overline{x}_2 x_3 \,\&\ldots\&\, x_{n-1}x_n \vee\ldots\vee \overline{x}_1\overline{x}_2\overline{x}_3 \,\&\ldots\&\, \overline{x}_{n-1}x_n. \quad (1)$$

Эта функция обращается в единицу на всех наборах, составляющих множество $N_h = \{(\underbrace{0,\ldots,0}_{s},\underbrace{1,\ldots,1}_{n-s}) \mid 1 \le s \le n-1\}$, и только на них.

Будем говорить, что множество M наборов из E_2^n (из $E_2^n(k)$) *обладает свойством* H тогда и только тогда, когда никакие два различных набора из M не могут быть получены один из другого транспозицией двух элементов. Максимальную мощность множества M, обладающего свойством H и содержащегося в $E_2^n \setminus \{(\tilde{0}^n), (\tilde{1}^n)\}$ (соответственно, в $E_2^n(k)$), обозначим через μ_n (соответственно, через $\mu_n(k)$). Очевидно, что

$$\mu_n = \sum_{k=1}^{n-1} \mu_n(k). \quad (2)$$

Лемма 1. *Всякий минимальный полный диагностический тест относительно произвольных перестановок переменных булевой функции* $h(\tilde{x}^n)$ *получается выбрасыванием из* $E_2^n \setminus \{(\tilde{0}^n),(\tilde{1}^n)\}$ *множества наборов, обладающего свойством* H.

Доказательство. Пусть в некоторый минимальный полный диагностический тест T относительно произвольных перестановок переменных булевой функции $h(\tilde{x}^n)$ не входят два различных набора $\tilde{\beta}$ и $\tilde{\gamma}$, лежащих в k-м слое E_2^n ($k \in \{1,2,\ldots,n-1\}$) и получающихся друг из друга транспозицией элементов, соответствующих переменным x_i и x_j. Пусть при этом все нулевые элементы набора $\tilde{\beta}$ соответствуют переменным $x_{\nu_1}, x_{\nu_2},\ldots, x_{\nu_{n-k-1}}, x_i$, а все нулевые элементы набора $\tilde{\gamma}$ соответствуют переменным $x_{\nu_1}, x_{\nu_2},\ldots, x_{\nu_{n-k-1}}, x_j$. Обозначим

$$\phi_1 = \begin{pmatrix} 1 & 2 & \dots & n-k-1 & n-k & n-k+1 & n-k+2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_{n-k-1} & i & j & \nu_{n-k+2} & \dots & \nu_n \end{pmatrix},$$

$$\phi_2 = \begin{pmatrix} 1 & 2 & \dots & n-k-1 & n-k & n-k+1 & n-k+2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_{n-k-1} & j & i & \nu_{n-k+2} & \dots & \nu_n \end{pmatrix},$$

а через ϕ_3 обозначим транспозицию элементов i и j. Заметим, что для подстановок ϕ_1, ϕ_2, ϕ_3 выполнено равенство: $\phi_2 = \phi_3(\phi_1)$. Пусть

$$\hat{h}'(x_1, x_2, \dots, x_n) = h(\zeta_{\phi_1}(x_1, x_2, \dots, x_n)) = h(x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_{n-k-1}}, x_i, x_j, x_{\nu_{n-k+2}}, \dots, x_{\nu_{n-1}}, x_{\nu_n}),$$

$$\hat{h}''(x_1, x_2, \dots, x_n) = h(\zeta_{\phi_2}(x_1, x_2, \dots, x_n)) = h(x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_{n-k-1}}, x_j, x_i, x_{\nu_{n-k+2}}, \dots, x_{\nu_{n-1}}, x_{\nu_n}).$$

Упорядочим (для простоты изложения) переменные $x_1, x_2, \dots, x_n$ следующим образом: $x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_{n-k-1}}, x_i, x_j, x_{\nu_{n-k+2}}, \dots, x_{\nu_{n-1}}, x_{\nu_n}$. При таком упорядочении переменных имеем:

$$\tilde{\beta} = (\underbrace{0,\dots,0}_{n-k},\underbrace{1,\dots,1}_{k}), \qquad \tilde{\gamma} = (\underbrace{0,\dots,0}_{n-k-1},1,0,\underbrace{1,\dots,1}_{k-1}),$$

и на основании представления (1):

$$N_{\hat{h}'} = \{(\underbrace{0,\dots,0}_{s},\underbrace{1,\dots,1}_{n-s}) \mid s \in N, s \le n-1\},$$

$$N_{\hat{h}''} = \{(\underbrace{0,\dots,0}_{s},\underbrace{1,\dots,1}_{n-s}), (\underbrace{0,\dots,0}_{n-k-1},1,0,\underbrace{1,\dots,1}_{k-1}) \mid s \in N, s \le n-1, s \ne n-k\}.$$

Сравнивая $N_{\hat{h}'}$ и $N_{\hat{h}''}$ и отмечая, что $\tilde{\beta} \in N_{\hat{h}'} \setminus N_{\hat{h}''}$, а $\tilde{\gamma} \in N_{\hat{h}''} \setminus N_{\hat{h}'}$, заключаем: $\hat{h}'(\tilde{x}^n)$ отличается от $\hat{h}''(\tilde{x}^n)$, и притом только на наборах $\tilde{\beta}$ и $\tilde{\gamma}$. Значит, если $\tilde{\beta}$ и $\tilde{\gamma}$ не входят в тест T, то на T невозможно отличить перестановочные функции $\hat{h}'$ и $\hat{h}''$, и T не является полным диагностическим тестом. Противоречие.

Докажем теперь, что всякое множество T наборов, полученное из $E_2^n \setminus \{(\tilde{0}^n), (\tilde{1}^n)\}$ выбрасыванием множества наборов, обладающего свойством H, образует полный диагностический тест для функции $h(\tilde{x}^n)$. Рассмотрим две произвольные перестановочные функции $h'(\tilde{x}^n) = h(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ и $h''(\tilde{x}^n) = h(x_{j_1}, x_{j_2}, \dots, x_{j_n})$. Пусть $i_1 = j_1$, $i_2 = j_2, \dots$, $i_{\eta-1} = j_{\eta-1}$, $i_\eta \ne j_\eta$ ($\eta \in \mathbb{N}$). Будем, не ограничивая общности, считать, что $i_\eta < j_\eta$. Рассмотрим набор $\tilde{\delta}$ такой, что на нем $x_{i_1} = x_{i_2} = \dots = x_{i_{\eta-1}} = x_{i_\eta} = 0$, а остальные переменные (в том числе x_{j_η}) обращаются в 1. Рассмотрим также набор $\tilde{\varepsilon}$, полученный из $\tilde{\delta}$ транспозицией элементов, соответствующих переменным i_η и j_η. Легко видеть, что каждый из наборов $\tilde{\delta}$, $\tilde{\varepsilon}$ отличает функции $h'(\tilde{x}^n)$ и $h''(\tilde{x}^n)$, а именно $h'(\tilde{\delta}) = 1$,

$h''(\tilde{\delta})=0$, $h'(\tilde{\varepsilon})=0$, $h''(\tilde{\varepsilon})=1$. А поскольку по крайней мере один из этих двух наборов обязан входить в T, то на множестве T можно отличить любую пару перестановочных функций. Значит, T – полный диагностический тест относительно произвольных перестановок переменных функции $h(\tilde{x}^n)$. Лемма доказана.

Лемма 2. *При* $n \geq 2$ *имеют место оценки:*

$$\frac{\binom{n}{k}}{k(n-k)+1} \leq \mu_n(k) \leq \frac{\binom{n}{k}}{\min(k,n-k)+1}.$$

Доказательство. Нижняя оценка. Пусть множество $M \subseteq E_2^n(k)$ обладает свойством H и при этом $|M| = \mu_n(k)$. Назовем *шаром* $\hat{S}_2^{n,k}(\tilde{\alpha}')$ *радиуса* 2 *в* $E_2^n(k)$ *с центром в наборе* $\tilde{\alpha}'$ множество тех и только тех наборов $\tilde{\alpha}'' \in E_2^n(k)$, для которых выполнено: $\rho(\tilde{\alpha}',\tilde{\alpha}'') \leq 2$. Очевидно, что если $\tilde{\alpha} \in M$, то в шаре радиуса 2 в $E_2^n(k)$ с центром в наборе $\tilde{\alpha}$ не лежат остальные наборы из M. Очевидно также, что совокупность всех шаров радиуса 2 в $E_2^n(k)$ с центрами в наборах из M покрывает слой $E_2^n(k)$ целиком, так как в противном случае непокрытый набор можно было бы добавить к M, что противоречило бы максимальности мощности M. Теперь нижняя оценка следует из того, что для всякого $\tilde{\alpha}' \in E_2^n(k)$: $|\hat{S}_2^{n,k}(\tilde{\alpha}')| = k(n-k)+1$.

Верхняя оценка. Для начала будем считать, что $k \leq n-k$. Пусть множество $M \subseteq E_2^n(k)$ обладает свойством H и при этом $|M| = p$. По принципу Дирихле существует такая переменная x_t, что на наборах множества M она обращается в единицу p_1 раз, где $p_1 \geq \frac{pk}{n}$ (тогда в нуль она обращается p_0 раз, где $p_0 = p - p_1 \leq \frac{p(n-k)}{n}$). Обозначим через $\hat{Q}_2^n(\tilde{\alpha}', x_t)$ множество различных наборов, каждый из которых получается из $\tilde{\alpha}'$ какой-либо транспозицией, в которой участвует переменная x_t (при этом заведомо предполагается, что $\tilde{\alpha}' \in \hat{Q}_2^n(\tilde{\alpha}', x_t)$). Легко видеть, что если $\tilde{\alpha}', \tilde{\alpha}'' \in M$, $\tilde{\alpha}' \neq \tilde{\alpha}''$, то $\hat{Q}_2^n(\tilde{\alpha}', x_t) \cap \hat{Q}_2^n(\tilde{\alpha}'', x_t) = \varnothing$. Далее, замечая, что для всякого набора $\tilde{\alpha}' \in M$ такого, что x_t на нем обращается в единицу, $|\hat{Q}_2^n(\tilde{\alpha}', x_t)| = n-k+1$, а для всякого набора $\tilde{\alpha}'' \in M$ такого, что x_t на нем обращается в нуль, $|\hat{Q}_2^n(\tilde{\alpha}'', x_t)| = k+1$, получаем очевидное неравенство:

$$p_1 \cdot (n-k+1) + p_0 \cdot (k+1) \leq \binom{n}{k},$$

откуда после несложных преобразований вытекает:

$$p + p_1(n-2k) + pk \le \binom{n}{k}, \qquad p \le \frac{\binom{n}{k}}{k+1}.$$

Проводя аналогичные рассуждения для случая $k > n-k$, окончательно выводим:

$$\mu_n(k) \le \frac{\binom{n}{k}}{\min(k, n-k)+1}, \tag{3}$$

что и доказывает лемму.

Лемма 3. *При* $n \ge 2$ *имеет место оценка:*

$$\mu_n \le \frac{4 \cdot 2^n}{n+1}.$$

Доказательство. Используя (2) и (3), получим:

$$\mu_n = \sum_{k=1}^{n-1} \mu_n(k) \le \sum_{k=0}^{n} \frac{\binom{n}{k}}{\min(k, n-k)+1} \le 2\sum_{k=0}^{\lceil n/2 \rceil} \frac{\binom{n}{k}}{k+1} \le 2\sum_{k=0}^{n} \frac{\binom{n}{k}}{k+1}.$$

Замечая, что, в силу бинома Ньютона,

$$\sum_{k=0}^{n} \frac{\binom{n}{k}}{k+1} \le \frac{2 \cdot 2^n}{n+1},$$

заключаем:

$$\mu_n \le \frac{4 \cdot 2^n}{n+1}.$$

Лемма доказана.

Верна следующая

Теорема 1. *При* $n \to \infty \quad l_{\mathfrak{S}}^{diagn}(n) \sim 2^n$.

Доказательство. Нижняя оценка

$$l_{\mathfrak{S}}^{diagn}(n) \ge 2^n - 2 - \mu_n \ge 2^n \cdot \left(1 - O\left(\tfrac{1}{n}\right)\right)$$

непосредственно вытекает из определения функции Шеннона $l_{\mathfrak{S}}^{diagn}(n)$ и из лемм 1, 2 и 3. Верхняя оценка $l_{\mathfrak{S}}^{diagn}(n) \le 2^n - n - 1$ тривиальна и следует из того, что в каждом слое любые две перестановочные функции различаются на четном числе наборов, а, следовательно, можно выбросить по одному набору из каждого слоя булева куба. Теорема доказана.

Теорема 2. *При* $n \in \mathbb{N} \quad l_{\mathfrak{L}}^{diagn}(n) = 2^n - 1$.

Доказательство. Нижняя оценка тривиальна и вытекает из рассмотрения функции $g(\tilde{x}^n) = x_1 x_2 \,\&\, \ldots \,\&\, x_n$. Так как $\mathfrak{L}(g)$ состоит из всех функций, обращающихся в единицу ровно на одном наборе, то

$l_{\mathfrak{L}}^{diagn}(g) \geq 2^n - 1$. Верхняя оценка также проста и следует из того, что для произвольной функции $f(\tilde{x}^n)$ расстояние Хемминга между столбцами значений любых двух неравных функций из $\mathfrak{L}(f)$ не меньше двух (поскольку эти столбцы одного веса), и для различения всех попарно неравных функций из $\mathfrak{L}(f)$ можно не использовать какой-то один набор из E_2^n. Теорема доказана.

О функциях Шеннона длин проверяющих тестов относительно произвольных перестановок переменных и относительно перестановок и отрицаний переменных

Распространим методику, предложенную Г. Р. Погосяном в [1] (см. также [2]) для оценивания сверху функции Шеннона длины проверяющего теста относительно произвольных инверсий переменных в булевой функции, на получение верхних оценок функции Шеннона $l_{\Gamma}^{detect}(n)$ в случае произвольной группы Γ биекций на E_2^n.

Пусть $f(\tilde{x}^n)$ – булева функция, Γ – группа (относительно композиции) биекций на E_2^n, $A \subseteq E_2^n$ – некоторое (возможно, пустое) множество наборов, $\zeta \in \Gamma$. Обозначим через $\zeta(A)$ множество наборов $\{\zeta(\tilde{\alpha}) \mid \tilde{\alpha} \in A\}$, а через $\Phi(f, A)$ – множество всех функций из $\Gamma(f)$, неотличимых от f на множестве наборов A (заметим, что $f = f_e \in \Phi(f, A)$). В частности, $\Phi(f, \varnothing) = \Gamma(f)$.

Лемма 4. *Пусть $f(\tilde{x}^n)$ – булева функция, Γ – группа (относительно композиции) биекций на E_2^n. Тогда для любого множества A_w $(A_w \subseteq E_2^n)$ такого, что $\Phi(f, A_w) \setminus \Phi(f, E_2^n) \neq \varnothing$, существует множество A_{w+1} $(A_{w+1} \subseteq E_2^n)$ такое, что $|A_{w+1}| = |A_w| + 1$ и*

$$|\Phi(f, A_{w+1})| \leq 0{,}5 \cdot |\Phi(f, A_w)|.$$

Доказательство. Пусть $\Gamma(f) = \{f_{\zeta_i}(\tilde{x}^n) \mid i = \overline{1,t}\}$, причем булевы функции $f_{\zeta_1} = f_e = f$, f_{ζ_2}, …, f_{ζ_s} лежат в $\Phi(f, A_w)$, а булевы функции $f_{\zeta_{s+1}}$, $f_{\zeta_{s+2}}$, …, f_{ζ_t} не лежат в $\Phi(f, A_w)$ $(1 \leq s \leq t)$. Так как $\Phi(f, A_w) \setminus \Phi(f, E_2^n) \neq \varnothing$, то найдутся набор $\tilde{\beta} \in E_2^n \setminus A_w$ и число $j \in \{1, 2, \ldots, s\}$ такие, что для функции $f_{\zeta_j}(\tilde{x}^n) \in \Phi(f, A_w)$ выполнено: $f_{\zeta_j}(\tilde{\beta}) \neq f(\tilde{\beta})$. Пусть среди чисел $f_{\zeta_1}(\tilde{\beta})$, $f_{\zeta_2}(\tilde{\beta})$, …, $f_{\zeta_s}(\tilde{\beta})$ значение $f(\tilde{\beta})$ встречается q раз.

Случай 1. Если $q \leq 0{,}5s$, то, полагая $A_{w+1} = A_w \cup \{\tilde{\beta}\}$, получаем: $|\Phi(f, A_{w+1})| \leq 0{,}5 \cdot |\Phi(f, A_w)|$, что и требовалось.

Случай 2. Пусть теперь $0{,}5s < q \leq s$. Так как для любого $i \in \{1, 2, \ldots, t\}$

$f_{\zeta_i(\zeta_j^{-1})}(\zeta_j(\tilde{x}^n)) = f_{\zeta_i}(\tilde{x}^n)$, то булевы функции $f_{\zeta_1(\zeta_j^{-1})}$, $f_{\zeta_2(\zeta_j^{-1})}$, …, $f_{\zeta_{j-1}(\zeta_j^{-1})}$, $f_{\zeta_j(\zeta_j^{-1})} = f_e = f$, $f_{\zeta_{j+1}(\zeta_j^{-1})}$, …, $f_{\zeta_s(\zeta_j^{-1})}$ лежат в $\Phi(f, \zeta_j(A_w))$, а булевы функции $f_{\zeta_{s+1}(\zeta_j^{-1})}$, $f_{\zeta_{s+2}(\zeta_j^{-1})}$, …, $f_{\zeta_t(\zeta_j^{-1})}$ не лежат в $\Phi(f, \zeta_j(A_w))$ (при этом, разумеется, $\Gamma(f) = \{f_{\zeta_i(\zeta_j^{-1})}(\tilde{x}^n) \mid i = \overline{1,t}\}$). Заметим, что среди чисел $f_{\zeta_1(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$, $f_{\zeta_2(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$, …, $f_{\zeta_s(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$ значение $f(\tilde{\beta})$ встречается q раз, и что

$$f(\zeta_j(\tilde{\beta})) = f_{\zeta_j(\zeta_j^{-1})}(\zeta_j(\tilde{\beta})) = f_{\zeta_j}(\zeta_j^{-1}(\zeta_j(\tilde{\beta}))) = f_{\zeta_j}(\tilde{\beta}) \neq f(\tilde{\beta}).$$

Значит, среди чисел $f_{\zeta_1(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$, $f_{\zeta_2(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$, …, $f_{\zeta_s(\zeta_j^{-1})}(\zeta_j(\tilde{\beta}))$ значение $f(\zeta_j(\tilde{\beta}))$ встречается $s-q$ раз, то есть, менее чем в половине случаев. Следовательно, полагая $A_{w+1} = \zeta_j(A_w) \cup \{\zeta_j(\tilde{\beta})\}$, получаем и в этом случае, что $|\Phi(f, A_{w+1})| \leq 0{,}5 \cdot |\Phi(f, A_w)|$. Лемма доказана.

Теорема 3. *Пусть $f(\tilde{x}^n)$ — булева функция, Γ – группа (относительно композиции) биекций на E_2^n. Тогда*

$$l_\Gamma^{detect}(f(\tilde{x}^n)) \leq \lceil \log_2 |\Gamma| \rceil.$$

Доказательство. Положим $A_0 = \varnothing$. Тогда $|\Phi(f, A_0)| = |\Gamma(f)| = |\Gamma|$. Применяя лемму 4 последовательно при $w = \overline{0, \lceil \log_2 |\Gamma| \rceil - 1}$, получим, что

$$\Phi(f, A_{\lceil \log_2 |\Gamma| \rceil}) \leq \frac{|\Gamma|}{2^{\lceil \log_2 |\Gamma| \rceil}} \leq 1,$$

откуда и следует утверждение теоремы.

Из этой теоремы мгновенно вытекает

Теорема 4. Пусть Γ – группа (относительно композиции) биекций на E_2^n. Тогда $l_\Gamma^{detect}(n) \leq \lceil \log_2 |\Gamma| \rceil$.

Применением формулы Стирлинга получаем

Следствие. $l_{\mathfrak{L}}^{detect}(n) \leq n \log_2 n (1 + o(1))$, $l_{\mathfrak{S}}^{detect}(n) \leq n \log_2 n (1 + o(1))$.

В работе [3] было показано, что нижней оценкой для функции Шеннона длины проверяющего теста относительно единичных транспозиций переменных в булевой функции, а, следовательно, и для функций Шеннона $l_{\mathfrak{L}}^{detect}(n)$, $l_{\mathfrak{S}}^{detect}(n)$ является величина $0{,}25n \log_2 n \,(1 + o(1))$. Значит, справедлива

Теорема 5. $l_{\mathfrak{L}}^{detect}(n) = \Theta(n \log_2 n)$, $l_{\mathfrak{S}}^{detect}(n) = \Theta(n \log_2 n)$.

Таким образом, в настоящей статье характер роста функции Шеннона длины теста относительно произвольных перестановок, а также перестановок и отрицаний переменных у булевой функции установлен на уровне асимптотики для случая диагностического теста и на уровне

порядка роста для случая проверяющего теста.

Автор выражает глубокую благодарность профессору Сергею Андреевичу Ложкину – за постановку задачи об асимптотике функции Шеннона длины диагностического теста относительно перестановок переменных и за внимание к работе, а также Алишеру Акрамовичу Икрамову – за ценные обсуждения по тематике статьи.

Литература

1. Погосян Г.Р. О проверяющих тестах для логических схем. М.: ВЦ АН СССР, 1982. 57 с.

2. Кудрявцев В.Б., Гасанов Э.Э., Долотова О.А., Погосян Г.Р. Теория тестирования логических устройств. М.: ФИЗМАТЛИТ, 2006. 160 с.

3. Глазунов Н.И., Горяшко А. П. Об оценках длин обнаруживающих тестов для классов неконстантных неисправностей входов комбинационных схем // Изв. АН СССР. Сер. «Техническая кибернетика». 1986. № 3. С. 197-200.