Е.В.Морозов

О ЕДИНИЧНЫХ ДИАГНОСТИЧЕСКИХ ТЕСТАХ ОТНОСИТЕЛЬНО СЛИПАНИЙ ПЕРЕМЕННЫХ В БУЛЕВЫХ ФУНКЦИЯХ*

В данной статье изучается поведение функций Шеннона длин диагностических тестов относительно слипаний переменных различных типов в булевых функциях. При стремящихся к бесконечности числе переменных устанавливаются: нижняя оценка функции Шеннона длины диагностического теста относительно всех допустимых слипаний; нижняя оценка функции Шеннона длины диагностического теста относительно дизъюнктивных слипаний; верхняя оценка функции Шеннона длины диагностического теста относительно линейных слипаний.

Будем говорить, что в булевой функции $f(x_1,...,x_n)$ произошло Φ *-слипание* переменных $x_{i_1},...,x_{i_k}$, если вместо исходной функции реализуется булева функция, полученная из нее подстановкой вместо каждой из переменных $x_{i_1},...,x_{i_k}$ функции $\varphi(x_{i_1},...,x_{i_k})$, где функция $\varphi\in\Phi$, φ будем также называть *функцией слипания*. Через $\Psi=\Psi_{n,f,\Phi}$ обозначим множество функций, в которое входит $f(x_1,...,x_n)$ и всевозможные булевы функции, получающиеся из $f(x_1,...,x_n)$ в результате Φ-слипаний. Φ-слипание называется $k-$кратным, если слипаются ровно k переменных. Множество наборов T назовем *диагностическим тестом для функции* $f(x_1,...,x_n)$, если для любой пары неравных функций из Ψ в T найдется набор, на котором эти функции принимают разные значения. Традиционным образом введем *функцию Шеннона длины диагностического теста относительно* Φ *-слипаний переменных* $L_\Phi(n)$ как максимум по всем булевым функциям длины минимального диагностического теста относительно Φ -слипаний. Введем специальные множества Φ : $\Phi_\vee$, содержащее все функции вида $g(x_1,...,x_k)=x_1\vee x_2\vee...\vee x_k$; Φ_{lin} , содержащее все функции вида $g(x_1,...,x_k)=x_1\oplus x_2\oplus...\oplus x_k\oplus\sigma$. Соответствущие множества функций неисправности будем обозначать через $\Psi_\vee,\Psi_{lin}$, а соответствующие функции Шеннона — $L_{\Phi_\vee}(n)$, $L_{\Phi_{lin}}(n)$. Также будем рассматривать Φ -слипания кратности не выше k , тогда:

* Работа выполнена при поддержке гранта РФФИ № 12-01-00964-а

$\Phi^k = \{g(x_1,...,x_i) \mid g(x_1,...,x_i) \in \Phi, i \le k\}$. Тогда множество функций неисправности обозначим через Ψ_{Φ^k}, а функцию Шеннона — через $L_{\Phi^k}(n)$.

Ранее рядом авторов изучались задачи, близкие к рассматриваемым в настоящей работе. Стоит отметить статьи В. Н. Носкова [1,2], в которых установлено точное значение функции Шеннона длины проверяющего теста и получены нетривиальные оценки функции Шеннона длины диагностического теста относительно константных неисправностей входов схем; препринт Г. Р. Погосяна [3], где найдена функция Шеннона длины проверяющего теста относительно дизъюнктивных слипаний; работы Д. С. Романова, И. А. Кузнецова [4] и Д. С. Романова [5], в которых установлены асимптотики функций Шеннона длин проверяющего и диагностического теста относительно локальных слипаний переменных в булевых функциях.

Теорема 1. *Пусть* Φ *— множество функций, такое, что* $\forall k\, \exists g(y_1,..., y_k) \in \Phi$. *Тогда для функции Шеннона* $L_\Phi(n)$ *при некоторой вещественной константе* C_1 *и при* $n \to \infty$ *справедлива нижняя оценка:*

$$L_\Phi(n) \ge \frac{C_1}{\sqrt[4]{n}} 2^{\frac{n}{2}} + o\left(\frac{2^{\frac{n}{2}}}{\sqrt[4]{n}}\right).$$

Доказательство. Заметим, что если в элементарной конъюнкции $x_1^{\sigma_1} x_2^{\sigma_2} ... x_m^{\sigma_m}$ произошло слипание, в котором участвуют переменные x_i, x_j такие, что $\sigma_i \ne \sigma_j$, то данная конъюнкция обратится в ноль, поскольку вместо переменных, входящих в конъюнкцию с разными степенями, будет подставлена одна и та же величина. Воспользуемся данным наблюдением и построим функцию, схожую с использованной Носковым [1] для константных неисправностей. Сначала будем предполагать, что $\forall k\, \exists g(y_1,..., y_k) \in \Phi$, не равная тождественному нулю. Опишем функцию, на которой достигается нижняя оценка:

$$h(x_1,...,x_n) = \bigvee_{\sigma_2+\sigma_3+...+\sigma_m = \left\lceil \frac{m}{2} \right\rceil - 1} x_1 x_2^{\sigma_2} ... x_m^{\sigma_m} x_{m+1}^{\delta_1(\tilde{\sigma}^m)} ... x_n^{\delta_{n-m}(\tilde{\sigma}^m)},$$

где векторы $\tilde{\delta}(\tilde{\sigma})$ выбираются так, что различным векторам $\tilde{\sigma}$ соответствуют разные $\tilde{\delta}(\tilde{\sigma})$. Найдем m, при котором число слагаемых в описанной ДНФ будет близко к максимальному.

Число всевозможных векторов $\tilde{\sigma}$, равное $C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$, тем больше, чем больше m. Число всевозможных векторов $\tilde{\delta}(\tilde{\sigma})$ равно 2^{n-m}, при этом должно выполняться неравенство $2^{n-m} \geq C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$. Используя известное асимптотическое равенство для биномиальных коэффициентов $(C_{2p}^{p} \sim \frac{2^{2p}}{\sqrt{\pi p}})$, при $m \to \infty$ получаем: $2^{n-m} \geq a\frac{2^{m-1}}{\sqrt{m}} + o(\frac{2^m}{\sqrt{m}})$, где a — некоторая константа.

Делим обе части на 2^{m-1}, логарифмируем, получаем: $n - 2m + 1 \geq \log\frac{a}{\sqrt{m}} + o(\log m)$ (здесь и далее логарифм берется по основанию 2). Представим $m = \frac{n}{2} + t$, тогда $2t \leq \log\sqrt{\frac{n}{2} + t} + o(\mathrm{logn})$. Учтем, что $t \leq \frac{n}{2}$, тогда получается, что $t \leq \frac{1}{2}\log n + o(\log n)$. Отсюда следует, что $2t \leq \log\sqrt{\frac{n}{2} + \frac{1}{2}\log n} + o(\log n)$. При $t \sim \frac{1}{2}\log n$ данное неравенство превращается в равенство. Итак, получаем, что $m \sim \frac{n}{2} + \frac{1}{2}\log n$.

Тождественный нуль получается из $h(x_1,...,x_n)$ слипанием всех переменных. Чтобы получить требуемую оценку, достаточно оценить снизу мощность множества наборов, отличающего нуль от других функций неисправности.

Предположим, что произошло слипание некоторых $\left\lceil \frac{m}{2} \right\rceil - 1$ переменных из $x_2,...,x_m$ и переменной x_1, функция слипания — некоторая отличная от нуля функция. Во всех слагаемых выбранной ДНФ, кроме одного, степени хотя бы двух неисправных переменных различны, следовательно только одно слагаемое может быть не равно тождественному нулю. Предположим, что данное слагаемое имеет вид: $x_1 x_2^{\sigma_1'} ... x_m^{\sigma_{m-1}'} x_{m+1}^{\delta_1'} ... x_n^{\delta_{n-m}'}$. Ясно, что оно не равно нулю только при $x_{m+1} = \delta_1', ..., x_n = \delta_{n-m}'$. Тогда каждому из рассматриваимых слипаний соответствуют различные вектора $\tilde{\delta}(\tilde{\sigma})$. Отсюда следует, что множества наборов, на которых соответствующие функции неисправности отличны от нуля, не пересекаются. Существование данных наборов обосновано тем, что среди функций слипания есть ненулевая функция.

Таким образом, чтобы отличить каждую из выбранных функций неисправности от тождественного нуля, потребуется столько же булевых наборов, сколько имеется функций неисправности. Их число равно $C_{m-1}^{\left\lceil \frac{m}{2} \right\rceil - 1}$. Поскольку можно выбрать $m \sim \frac{n}{2} + \frac{1}{2}\log n$, снова воспользовавшись асимптотическим равенством для биномиальных коэффициентов, получаем требуемую оценку.

Если же при каком-то n в множестве Φ не будет необходимой отличной от нуля функции, рассуждая двойственным образом, получаем нужную оценку. Теорема доказана.

Далее через $f_{x_{i_1},...,x_{i_k}}^{g(x_{i_1},...,x_{i_k})}(x_1,...,x_n)$ будем обозначать функцию неисправности, получающуюся из $f(x_1,...,x_n)$ в результате слипания переменных $x_{i_1},...,x_{i_k}$ с функцией слипания $g(x_{i_1},...,x_{i_k})$. Для набора $\tilde{\alpha}$ через $|\tilde{\alpha}|$ обозначим число единиц в данном наборе.

Теорема 2. *Для функции Шеннона* $L_{\Phi_\vee}(n)$ *при некоторой вещественной константе* C_2 *и при* $n \to \infty$ *справедлива нижняя оценка:* $L_{\Phi_\vee}(n) \geq \frac{C_2}{\sqrt{n}} 2^n + o(\frac{2^n}{\sqrt{n}})$.

Доказательство. В нижеследующих рассуждениях будем говорить, что набор $\tilde{\alpha} = (\alpha_1,...,\alpha_n)$ *переходит* в набор $\tilde{\beta} = (\beta_1,...,\beta_n)$ в результате слипания переменных $x_{i_1},...,x_{i_p}$, если $\beta_j = \alpha_{i_1} \vee \alpha_{i_2} \vee ... \vee \alpha_{i_p}$ при $j \in \{i_1,...,i_p\}$ и $\beta_j = \alpha_j$ в противном случае.

Рассмотрим сначала нечетное n. Тогда $\left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{n}{2} \right\rfloor + 1$. Возьмем функцию $h(x_1,...,x_n)$, равную единице на всех наборах $\tilde{\alpha}$, для которых $|\tilde{\alpha}| = \left\lfloor \frac{n}{2} \right\rfloor$ и нулю на всех остальных. Сузим класс возможных неисправностей до слипаний кратности $\left\lceil \frac{n}{2} \right\rceil$. В результате дизъюнктивного слипания переменных набор $\tilde{\beta}$ переходит в набор $\tilde{\beta}'$ так, что $|\tilde{\beta}'| \geq |\tilde{\beta}|$.

Поэтому если $|\tilde{\beta}|\geq\left\lceil \frac{n}{2} \right\rceil$, то на наборе $\tilde{\beta}$ значение любой из возможных функций неисправности равно нулю. Если $|\tilde{\beta}|<\left\lfloor \frac{n}{2} \right\rfloor$ и в слипании участвуют только переменные, на местах которых в наборе $\tilde{\beta}$ стоит ноль, данный набор не изменится и значение функции неисправности будет равно нулю. А если в слипании участвует хотя бы одна переменная, значение которой на наборе $\tilde{\beta}$ равно единице, тогда он перейдет в некоторый набор $\tilde{\beta}'$, для которого верно $|\tilde{\beta}'|\geq\left\lceil \frac{n}{2} \right\rceil$, в силу того, что кратность рассматриваемых слипаний равна $\left\lceil \frac{n}{2} \right\rceil$. Поэтому значение функций неисправности также будет равно нулю. Поэтому далее будем рассматривать только наборы $\tilde{\alpha}:|\tilde{\alpha}|=\left\lfloor \frac{n}{2} \right\rfloor$. Пусть $X'=\left\{x_{i_1},\ldots,x_{i_{\left\lceil \frac{n}{2} \right\rceil}}\right\}, X''=\left\{x_{j_1},\ldots,x_{j_{\left\lceil \frac{n}{2} \right\rceil}}\right\}$, $X'\neq X''$. Тогда $h^{X'}_{x_{i_1}\vee\ldots\vee x_{i_{\left\lceil \frac{n}{2} \right\rceil}}}$ и $h^{X''}_{x_{j_1}\vee\ldots\vee x_{j_{\left\lceil \frac{n}{2} \right\rceil}}}$ — две различные функции неисправности.

Заметим, что если в наборе $\tilde{\alpha}$ есть хотя бы одна единица в позициях, соответствующих переменным из X' и хотя бы одна единица в позициях, соотвествующих переменных из X'', то обе функции будут равны нулю на данном наборе в силу кратности рассматриваемых слипаний. Тогда функции могут отличаться от нуля только на наборах, у которых в позициях $i_1,\ldots,i_{\left\lceil \frac{n}{2} \right\rceil}$ или $j_1,\ldots,j_{\left\lceil \frac{n}{2} \right\rceil}$ стоят все нули. Поскольку рассматриваются только наборы, в которых ровно $\left\lfloor \frac{n}{2} \right\rfloor$ единиц, получаем, что данные функции различаются всего на двух наборах.

Пусть в тест не входят некоторые два набора $\tilde{\alpha}'$ и $\tilde{\alpha}''$, для которых $|\tilde{\alpha}'|=|\tilde{\alpha}''|=\left\lfloor \frac{n}{2} \right\rfloor$. Тогда слипание переменных, соответствующих нулям в наборе $\tilde{\alpha}'$ и слипание переменных, соответствующих нулям в наборе $\tilde{\alpha}''$, не будут отличены друг от друга.

Отсюда следует, что в тест входит не менее, чем $C_n^{\left\lfloor \frac{n}{2} \right\rfloor}-1$ наборов. Оценив данное выражение снизу и устремив n к бесконечности, получаем: $L_{\Phi_\vee}(n) \geq C_n^{\left\lfloor \frac{n}{2} \right\rfloor}-1 > C_{n-1}^{\frac{n-1}{2}} \sim \sqrt{\frac{2}{\pi}}\frac{2^{n-1}}{\sqrt{n-1}} \sim \frac{1}{\sqrt{2\pi}}\frac{2^n}{\sqrt{n}}$. Для четных n, рассматривая функцию $h(x_1,...,x_n)$, равную единице только на наборых $\tilde{\alpha}:|\tilde{\alpha}|=\frac{n}{2}-1$, и слипания кратности $\frac{n}{2}+1$, аналогично получаем нижнюю оценку длины теста: $L_{\Phi_\vee}(n) \geq C_n^{\frac{n}{2}-1}-1 > C_{n-2}^{\frac{n}{2}-1} \sim \sqrt{\frac{2}{\pi}}\frac{2^{n-2}}{\sqrt{n-1}} \sim \frac{1}{2\sqrt{2\pi}}\frac{2^n}{\sqrt{n}}$.

Теорема доказана.

Дадим далее некоторые определения и докажем леммы, которые понадобятся при выводе верхней оценки для линейных слипаний.

Пусть дана функция $t(x_1,...,x_n)$. *Проверяющей парой* для переменных x_i, x_j, $i \neq j$ назовем пару наборов $\tilde{\alpha}=(\alpha_1,...,\alpha_n), \tilde{\beta}=(\beta_1,...,\beta_n)$, таких что $h(\tilde{\alpha}) \neq h(\tilde{\beta})$ и при $k \in \{i,j\}$ $\alpha_k \neq \beta_k$, а при всех остальных k имеет место равенство: $\alpha_k = \beta_k$.

Пусть $\tilde{\alpha}$ — некоторый n-мерный вектор, каждая компонента которого может принимать одно из значений: $\{0,1,2\}$. *Гранью* в кубе B^n будем называть множество булевых наборов этого куба, i-я компонента которых равна α_i, если α_i равна нулю или единице, и принимает произвольное значение, если $\alpha_i = 2$. Переменные, соответствующие двойкам в наборе $\tilde{\alpha}$, назовем *свободными переменными* грани, а их число — *размерностью* грани. Если в множестве булевых наборов Q содержится набор, принадлежащий некоторой грани в булевом кубе, будем говорить, что множество Q *протыкает* данную грань.

Пусть Z — подмножество множества переменных $\{x_1,...,x_n\}$, $\tilde{\alpha},\tilde{\beta}$ — n-мерные булевы наборы. Будем обозначать: $\tilde{\alpha} =_Z \tilde{\beta}$, если разряды данных наборов, соответствующих переменным из Z, совпадают, $|\tilde{\alpha}|_Z = m$, если в разрядах набора $\tilde{\alpha}$ на местах переменных из Z стоит ровно m единиц.

Расстоянием Хемминга $\rho(\tilde{\alpha},\tilde{\beta})$ между булевым наборами $\tilde{\alpha}$ и $\tilde{\beta}$ называется число разрядов, в которых эти наборы различаются.

Совокупность наборов $\tilde{\alpha}$, для которых $|\tilde{\alpha}|=k$, назовем k*-м слоем* булева куба. Назовем функцию *симметрической*, если ее значения совпадают на любых двух наборах, принадлежащих одному слою булева куба.

Введем бинарное отношение R_t на множестве переменных функции $t(\tilde{x}^n)$ следующим образом. Всегда верно, что $x_i R_t x_i$. Если $i \neq j$, то $x_i R_t x_j$ тогда и только тогда, когда для переменных x_i, x_j функции $t(\tilde{x}^n)$ не существует проверяющей пары.

Лемма 1. *R_t есть отношение эквивалентности.*

Доказательство. Очевидно, данное отношение рефлексивно и симметрично. Докажем, что оно транзитивно. Пусть i, j, k — попарно различные числа. Тогда если нет проверяющих пар для x_i, x_j и x_i, x_k, то нет проверяющей пары и для переменных x_j, x_k. Положим для удобства $i=1$, $j=2$, $k=3$, $\tilde{\gamma}=(\gamma_4,\gamma_5,...,\gamma_n)$ и выпишем соотношения, следующие из отсутствия проверяющих пар для x_1, x_2 и x_1, x_3, из которых будет следовать требуемое утверждение:

$t(1,1,0,\tilde{\gamma}) = t(0,0,0,\tilde{\gamma}) = t(1,0,1,\tilde{\gamma}) = t(0,1,1,\tilde{\gamma})$,

$t(0,0,1,\tilde{\gamma}) = t(1,1,1,\tilde{\gamma}) = t(0,1,0,\tilde{\gamma}) = t(1,0,0,\tilde{\gamma})$.

Если среди i, j, k есть равные числа, то очевидно, что из $x_i R_f x_j$, $x_j R_f x_k$ следует $x_i R_f x_k$.

Таким образом, получаем, что R_t — отношение эквивалентности.

Лемма доказана.

Переменные $x_1,...,x_n$ разбиваются на непересекающиеся классы эквивалентности по отношению R_t. Каждый класс эквивалентности назовем *множеством линейности*.

Лемма 2. *Пусть ни для какой пары переменных функции $t(x_1,...,x_m)$ не существует проверяющей пары. Тогда $t(x_1,...,x_m)$ есть одна из четырех функций:* $0, 1, x_1 \oplus x_2 \oplus ... \oplus x_m, x_1 \oplus x_2 \oplus ... \oplus x_m \oplus 1$.

Доказательство. Наборы проверяющей пары отличаются в двух разрядах. Следовательно, если взять произвольный набор $\tilde{\alpha}$, у которого в i-й позиции стоит 0, а в j-й позиции стоит 1, и набор $\tilde{\beta}$, отличающийся от него ровно в этих разрядах, значения функции на данных наборах будут одинаковы. Получаем, что $t(x_1,...,x_m)$ — симметрическая функция. Кроме того, если в произвольном наборе $\tilde{\gamma}$ в позициях i и j стоят нули, а набор

$\tilde{\delta}$ отличается от него ровно в этих двух разрядах, значения функции на данных наборах также будут одинаковы. Следовательно, функция $t(x_1,...,x_m)$ на всех четных слоях булева куба принимает некоторое значение a, а на всех нечетных — некоторое значение b. Таких функций всего четыре: $0, 1, x_1 \oplus x_2 \oplus ... \oplus x_m, x_1 \oplus x_2 \oplus ... \oplus x_m \oplus 1$

Лемма доказана.

Лемма 3. *Пусть* F_1 *— множество функций неисправности, для которых длина диагностического теста равна* l_1, F_2 *— множество функций неисправности, для которых длина диагностического теста равна* l_1. *Тогда для множества* $F = F_1 \cup F_2$ *существует диагностический тест длины не более, чем* $l_1 + l_2 + \min\{|F_1|,|F_2|\}$

Доказательство. Пусть T_1 — диагностический тест длины l_1 для F_1, T_2 — диагностический тест длины l_2 для F_2. Положим $T' = T_1 \cup T_2$ и $|F_1| \le |F_2|$. Тогда на множестве T' функции из F_1 отличены друг от друга, функции из F_2 отличены друг от друга, каждая функция из F_1 неотличима не более, чем от одной функции из F_2. Первые два утверждения очевидны, покажем третье. Пусть это не так и некоторая функция $f_1 \in F_2$ неотличима от $f_2^1, f_2^2 \in F_2$, $f_2^1 \ne f_2^2$. В множестве T' существует набор $\tilde{\alpha}$: $f_2^1(\tilde{\alpha}) \ne f_2^2(\tilde{\alpha})$. Тогда на данном наборе f_1 отличима от одной из функций f_2^1, f_2^2. Получаем противоречие. Отсюда следует, что для того, чтобы множество T' было диагностиеским тестом для F, к нему достаточно добавить не более, чем $|F_1|$ наборов.

Лемма доказана.

Зафиксируем некоторое число k. Через $R(k)$ обозначим множество наборов, протыкающее все грани булева куба размерности k. По лемме о протыкании [6] можно построить множество $R(k)$ такое, что $|R(k)| \le (n+1)2^{n-k}$ Легко видеть, что данное множество является протыкающим и для всех граней размерности, большей k. Через $T_1(k)$ обозначим множество, состоящее из наборов множества $R(k)$ и всех наборах, находящися от них на расстоянии, не больше 3. Тогда

$$|T_1(k)| \le (n+1)(1 + C_n^1 + C_n^2 + C_n^3)2^{n-k} \le \frac{n^4}{2}2^{n-k} + o(\mathrm{n}^4 2^{n-k})$$

Лемма 4. *Пусть* $Z \subseteq X$, $|Z| \ge k$, $h(x_1,...,x_n)$ *— булева функция, у* *которой ни для каких двух переменных из* Z *нет проверяющей пары. Тогда если для переменных* x_r, x_s *у* $h(x_1,...,x_n)$ *существуют проверяющие пары, то хотя бы одна проверяющая пара для них содержится в множестве* $T_1(k)$.

Доказательство. Действительно, пусть $\tilde{\alpha}_1$ и $\tilde{\alpha}_2$ — проверяющая пара для переменных x_r и x_s. Множество наборов, совпадающих с $\tilde{\alpha}_1$ в разрядах, соответствующих переменным из $X \setminus Z$, образует грань в булевом кубе размерности $|Z| \geq k$, поэтому в $R(k)$ есть набор $\tilde{\beta}_1$, ее протыкающий.

Пусть $|\tilde{\beta}_1|_Z = |\tilde{\alpha}_1|_Z \pmod 2$. Тогда $h(\tilde{\beta}_1) = h(\tilde{\alpha}_1)$. Это следует из леммы 2, поскольку, если зафиксировать значения переменных из множества $X \setminus Z$, будет реализовываться симметрическая функция, значения которой определяются только четностью числа единиц входного набора. Инвертируем в наборе $\tilde{\beta}_1$ разряды с номерами r и s, получим набор $\tilde{\beta}_2$. Рассуждая аналогично, получаем, что $h(\tilde{\beta}_2) = h(\tilde{\alpha}_2)$, а следовательно, $\tilde{\beta}_1, \tilde{\beta}_2$ — проверяющая пара для переменных x_r, x_s функции $h(x_1,...,x_n)$. Набор $\tilde{\beta}_1$ лежит в $R(k)$, поэтому лежит и в $T_1(k)$. Набор $\tilde{\beta}_2$ находится от него на расстоянии 2, поэтому также лежит в $T_1(k)$

Если $|\tilde{\beta}_1|_Z \neq |\tilde{\alpha}_1|_Z \pmod 2$, выберем произвольную переменную x_j из $Z \setminus \{x_r \cup x_s\}$ и, инвертировав разряд j в наборе $\tilde{\beta}_1$, получим набор $\tilde{\beta}'_1$, а, инвертировав в $\tilde{\beta}'_1$ разряды r и s, получим $\tilde{\beta}'_2$. Данные наборы являются проверяющей парой для переменных x_r, x_s функции $h(x_1,...,x_n)$ (устанавливается аналогично). Данные наборы лежат в T', поскольку $\rho(\tilde{\beta}_1, \tilde{\beta}'_1) = 1$, а $\rho(\tilde{\beta}_1, \tilde{\beta}'_2) = 3$.

Лемма доказана.

Лемма 5. *Пусть* $Z \in X$, $|Z| \geq k$. *Пусть у функций* $h_1(x_1,...,x_n), h(x_1,...,x_n)$ *нет проверяющих пар ни для каких двух переменных из* Z *и* $h_1(x_1,...,x_n) \neq h(x_1,...,x_n)$. *Тогда в множестве* $T_1(k)$ *существует набор, на котором данные функции неравны.*

Доказательство. Пусть $h_1(\tilde{\alpha}) \neq h_2(\tilde{\alpha})$. Все наборы, отличающиеся от $\tilde{\alpha}$ в разрядах, соответствующих переменным из Z, образуют грань размерности $|Z|$, поэтому во множестве T содержится набор $\tilde{\beta}$, ее протыкающий. Допустим, что $|\tilde{\alpha}|_Z = |\tilde{\beta}|_Z \pmod 2$. Тогда аналогично рассуждениям третьей леммы получаем: $h_1(\tilde{\beta}) = h_1(\tilde{\alpha}) \neq h_2(\tilde{\alpha}) = h_2(\tilde{\beta})$. Если же $|\tilde{\alpha}|_Z \neq |\tilde{\beta}|_Z \pmod 2$, то вместо набора $\tilde{\beta}$ возьмем из множества $T_1(k)$ набор, соседний ему по какой-либо переменной из Z и, повторив проведенные рассуждения, получим, что данный набор различает функции $h_1(x_1,...,x_n)$ и $h_2(x_1,...,x_n)$.

Лемма доказана.

Теорема 3. *Для функции Шеннона* $L_{\Phi_{lin}}(n)$ *при* $n \to \infty$ *справедлива верхняя оценка* $L_{\Phi_{lin}}(n) \le n^4 2^{0.773n} + o(n^4 2^{0.773n})$.

Доказательство. Разобьем доказательство на две части. На первом шаге выберем некоторое натуральное число $k \ge \left\lfloor \frac{n}{2} \right\rfloor$ и покажем, что множество наборов $T_1(k)$, различает все слипания кратности более, чем k.

Пусть $X' = \left\{x_{i_1},...,x_{i_p}\right\}$ и $X''\left\{x_{j_1},...,x_{j_q}\right\}$ — несовпадающие подмножества множества переменных $\{x_1,...,x_n\}$. Рассмотрим функции неисправности $f_{X'}^{g_1(x_{i_1},...,x_{i_p})}$ и $f_{X''}^{g_2(x_{j_1},...,x_{j_q})}$, где $g_1(x_{i_1},...,x_{i_p}) \in \Phi_{lin}$ и $g_2(x_{j_1},...,x_{j_q}) \in \Phi_{lin}$. Предположим, что $x_r, x_s \in X''$ и у функции $f_{X'}^{g_1(x_{i_1},...,x_{i_p})}$ есть проверяющая пара для этих переменных. Очевидно, что ни для каких переменных из X' у функции $f_{X'}^{g_1(x_{i_1},...,x_{i_p})}$ нет проверяющей пары, поэтому по лемме 4 получаем, что для переменных x_r, x_s у функции $f_{X'}^{g_1(x_{i_1},...,x_{i_p})}$ есть проверяющая пара в множестве $T_1(k)$. На одном из наборов проверяющей пары функции различаются.

Если ни для какой пары переменных их X'' у функции $f_{X'}^{g_1(x_{i_1},...,x_{i_p})}$ нет проверяющей пары, то мы можем применить лемму 5, взяв X'' в качестве множества Z. Тогда если выбранные функции неисправности различаются, в $T_1(k)$ имеется набор, на котором они неравны.

Рассмотрим теперь слипания кратности не выше k. Число всевозможных функций неисправности не превышает $2(1 + C_n^1 + ... + C_n^k) \le 2kC_n^k$. Из тривиальной верхней оценки длины диагностического теста следует, что мощность множества наборов $T_2(k)$, различающего выбранные функции неисправностей, ограничена сверху числом $2kC_n^k - 1$.

Таким образом, все слипания кратности выше k отличены друг от друга, и все слипания кратности не выше k различены между собой. Если T — искомый диагностический тест, то, применяя лемму 3, получаем верхнюю оценку мощности множества T : $|T| \le 2kC_n^k + \frac{n^4}{2} 2^{n-k} + \min(2kC_n^k, 2^{n+1} - 2kC_n^k)$.

Введем функцию $H(a) = -a\log a - (1-a)\log(1-a)$. Применяя известное неравенство $C_n^r \le 2^{nH(\frac{r}{n})}$ при $r \le \frac{n}{2}$, выбирая $k = \lceil 0,227n \rceil$ и пользуясь таблицей значений для функции $H(a)$, получаем, что при $n \to \infty$ верно:

$$|T| \le 2kC_n^k + \frac{n^4}{2} 2^{n-k} + \min\left\{2kC_n^k, 2^{n+1} - 2kC_n^k)\right\} \le n2^{0.773n} + \frac{n^4}{2} 2^{0.773n} + n2^{0.773n}$$
$$\le n^4 2^{0.773n}$$

Теорема доказана.

Литература

1. Носков В. Н. Диагностические тесты для входов логических устройств // Дискретный анализ. Новосибирск: ИМ СО АН СССР, 1974. № 26. С. 72-83.
2. Носков В. Н. О сложности тестов, контролирующих работу входов логических схем // Дискретный анализ. Новосибирск: ИМ СО АН СССР, 1975. № 27. С. 23-51.
3. Погосян Г. Р. О проверяющих тестах для логических схем. М.: ВЦ АН СССР, 1982. 57 с.
4. Кузнецов И. А., Романов Д. С. О полных проверяющих тестах относительно локальных слипаний переменных в булевых функциях // Ученые записки Казанского государственного университета. Серия «Физико-математические науки», 2009. Том 151, книга 2. Стр. 90-97.
5. Romanov D. S. Diagnostic tests for local coalescences of variables in Boolean functions // Computation mathematics and modeling. 2012, № 1, с. 72-79.
6. Нечипорук Э.И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР, 1965, Том 163, № 1, с. 40-42.