О проверяющих тестах относительно локальных перестановок входов схем

М. А. Лопунов[1]

В работе установлен порядок роста функции Шеннона длины проверяющего теста относительно источника неисправностей, который может произвольным образом менять местами любые k подряд идущих входов схемы.

Ключевые слова: проверяющий тест, тесты на входах СФЭ, функция Шеннона, перестановки.

1. Введение

В данной работе исследуется поведение функции Шеннона длины проверяющего теста для неисправностей, происходящих на входах схем, а именно будет рассматриваться источник, который может произвольным образом менять местами подряд идущие входы схемы в рамках фиксированных границ. В работе [1] было доказано, что нижней оценкой для функции Шеннона длины проверяющего теста относительно единичных транспозиций переменных в булевой функции является величина $0,25n\log_2 n(1+o(1))$. В работе [2] доказано, что верхней оценкой для данной функции Шеннона является величина $n\log_2 n(1+o(1))$. Таким образом, было установлено, что данная функция Шеннона ведёт себя как $\Theta(n\log n)$.

2. Основные понятия и формулировка результата

Рассматриваются проверяющие тесты для входов схем из функциональных элементов (СФЭ) с одним выходом. Множество наборов T булева куба называется *проверяющим тестом* для СФЭ Σ относительно источника неисправностей U, если любая неисправная схема, полученная под действием этого источника из исходной схемы, может быть функционально отличима хотя бы на одном наборе из этого множества от исходной схемы. Множество T с минимальным числом наборов называется *минимальным тестом* для Σ относительно U. *Длиной теста для булевой функции* f будем называть наименьший по мощности минимальный

[1] *Лопунов Михаил Александрович* — студент каф. математической кибернетики ф-та ВМК МГУ, e-mail: miklop07@gmail.com.

Lopunov Mikhail Alexandrovich — student, Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, Chair of Mathematical Cybernetics.

тест среди всех СФЭ, реализующих f. *Функцией Шеннона длины проверяющего теста* называется функция $l^{detect}(n)$, равная максимуму длин проверяющих тестов для булевых функций по всем булевым функциям от n переменных.

В данной работе рассматривается источник неисправностей U_k, который может произвольным образом менять местами любые k подряд идущих входов схемы. Обозначим через $l_k^{detect}(n)$ функцию Шеннона длины проверяющего теста относительно источника неисправностей U_k. В результате доказаны верхняя и нижняя оценки для $l_k^{detect}(n)$, устанавливающие порядок роста.

Теорема 1. *Пусть k, n — натуральные числа, $2 \le k \le n$, $n \to \infty$, $k = k(n)$. Тогда имеет место неравенства $\frac{1}{16} n \log_2 k \le l_{k(n)}^{detect}(n) \le 6n \log_2 k$.*

Доказательство. *Верхняя оценка.* Рассмотрим произвольную булеву функцию (БФ) $f(x_1, \ldots, x_n) \in P_2(n)$. Сначала докажем оценку для $2 \le k < \lfloor \frac{n}{2} \rfloor$. Рассмотрим $\lfloor \frac{n}{2k} \rfloor + \lfloor \frac{n-k}{2k} \rfloor$ наборов переменных БФ f вида $(x_{ik+1}, \ldots, x_{ik+2k})$, где $i \in \{0, 1, \ldots, \lfloor \frac{n}{2k} \rfloor + \lfloor \frac{n-k}{2k} \rfloor - 1\}$. Обозначим множество всех таких наборов через M. Если n не кратно k, добавим в M набор $\delta = (x_t, \ldots, x_n), t = (\lfloor \frac{n}{2k} \rfloor + \lfloor \frac{n-k}{2k} \rfloor)k + 1$. Далее, рассмотрим произвольный набор $x' \in M$ и множество $S_{x'}$ всевозможных перестановок переменных $(x_1, \ldots, x_n)$, которые могут менять местами только переменные x'. Введём множество $W_{f,x'}$ всех БФ, получающихся из f путём перестановок из $S_{x'}$ входных переменных. Очевидно, что множество перестановок $S_{x'}$ индуцирует на E_2^n группу биекций относительно композиции. Используем результат, полученный в работе [2]. Тогда f можно отличить от любой БФ из $W_{f,x'}$, используя $\lceil \log_2 |S_{x'}| \rceil = \lceil \log_2((2k)!) \rceil \le 2k \log_2(2k) \le 4k \log_2 k$ наборов. Видно, что

$$|M| \le \left\lfloor \frac{n}{2k} \right\rfloor + \left\lfloor \frac{n-k}{2k} \right\rfloor + 1 \le \frac{2n+k}{2k} \le \frac{3n}{2k}.$$

Поэтому, чтобы отличить f от любой БФ из объединения $W_{f,x'}$ по всем x' из M, используем не более $|M| 4k \log k \le 6n \log_2 k$ наборов. Обозначим множество этих наборов через T.

Далее, рассмотрим произвольную БФ f_φ, которая получается из f под действием источника неисправностей U_k и отличается от f хотя бы на одном наборе. Из построения T видно, что $\exists \tilde{\beta} \in T$ такой, что $f(\tilde{\beta}) \ne f_\varphi(\tilde{\beta})$. Следовательно, T является тестом для f.

При $\lfloor \frac{n}{2} \rfloor \le k \le n$ также воспользуемся результатом [2] для $k = n$. Очевидно, что с помощью такого теста T также можно отличить любые неисправности, связанные с U_k при $\lfloor \frac{n}{2} \rfloor \le k \le n$. Тогда

$$|T| \le \lceil n \log_2 n \rceil \le n \log_2(2n) \le n \log_2(4k+2) \le 6n \log_2 k.$$

Таким образом, доказано, что $l_k^{detect}(n) \leq 6n \log_2 k$.

Нижняя оценка. Воспользуемся идеей, предложенной в работе [1]. Будем строить функцию для $k + \log_2 k \leq n$. Если $k + \log_2 k > n$, то для таких параметров k и n будем строить функцию как для параметров k' и n соответственно, где k' — такое наибольшее возможное целое число, что $2 \leq k'$ и $k' + \log_2 k' \leq n$. Тогда останется нерассмотренным случай $k = n = 2$, но в этом случае положим результатом построения БФ $f(x_1, x_2) = (0, 0, 1, 0)$ с тестом длины 1.

Построим характеристическое множество N_f БФ f. Пусть m — остаток от деления n на k. Также определим число δ' равное m, если $m \geq \lfloor \log_2 k \rfloor - 1$ и равное $k + m$ иначе. Построим множества $K_i \subseteq E_2^n$ для всех i из $I = \big\{1, 2, \ldots, \lfloor \log_2 k \rfloor\big\}$. Опишем наборы $\tilde{\omega}$, из которых будет состоять множество K_i. У всех наборов $\tilde{\omega}$ координаты с номерами, большими $n - i + 1$, будут равны единице. Положим координаты с номерами $n - \delta' + 1, n - \delta' + 2, \ldots, n - i + 1$ равными нулю. Среди первых $n - \delta'$ будет ровно одна единица, остальные координаты положим равными нулю. Эта единица может стоять на любых позициях с номерами $1 + a2^i, 2 + a2^i, \ldots, 2^{i-1} + a2^i$, где a может быть любым целым неотрицательным числом, не превосходящим значение $\lfloor \frac{n-\delta'}{2^i} \rfloor - 1$. Таким образом, K_i состоит из всевозможных наборов $\tilde{\omega} \in E_2^n$, описанных выше, и только из них. Тогда положим N_f как объединение всех K_i по всем i из I. Пусть $T = N_f$.

Покажем, что T является тестом для f. Рассмотрим произвольную перестановку ζ переменных $x_1, \ldots, x_n$ такую, что $f_\zeta = f(\zeta(x_1, \ldots, x_n)) \neq f$. Тогда $N_f \neq N_{f_\zeta}$, но $|N_f| = |N_{f_\zeta}|$. Значит, $\exists \hat{\sigma} \in N_f = T : f(\hat{\sigma}) \neq f_\zeta(\hat{\sigma})$.

Теперь докажем минимальность T. Зафиксируем произвольный набор $\tilde{\Delta} \in N_f$. Пусть i — число единиц среди последних δ' координат. По построению в $\tilde{\Delta}$ на первых $n - \delta'$ позициях ровно одна единица. Обозначим через q позицию с единицей. Обозначим через $\zeta_{\tilde{\Delta}} : E_2^n \to E_2^n$ транспозицию элементов $\tilde{\Delta}$ на позициях q и $q + 2^i$. Очевидно, что f и $f_{\zeta_{\tilde{\Delta}}}$ отличимы на двух наборах: $\tilde{\Delta}$ и $\zeta_{\tilde{\Delta}}(\tilde{\Delta})$. Заметим, что $\{\tilde{\Delta}, \zeta_{\tilde{\Delta}}(\tilde{\Delta})\} \cap \{\tilde{\Delta}', \zeta_{\text{ﬃ}\Delta'}(\tilde{\Delta}')\} = \varnothing$ для любого $\tilde{\Delta}' \in N_f : \tilde{\Delta}' \neq \tilde{\Delta}$. Тогда f можно отличить от $f_{\zeta_{\tilde{\Delta}}}$ только на $\tilde{\Delta}$ и $\zeta_{\tilde{\Delta}}(\tilde{\Delta})$, но $\tilde{\Delta}$ уже есть в T.

Оценим длину T. Сначала проведём оценку для $n = 2^r + r - 1, r \in \mathbb{N}$. Заметим, что $\log_2 n = \log_2(2^r + r - 1) = r + \log_2\left(1 + \frac{r-1}{2^r}\right) < r + 1$. Тогда $r - 1 > \log_2 n - 2$. Всего множеств K_i ровно $\lfloor \log_2 k \rfloor$. Каждое из них имеет мощность, равную 2^{r-1}. Тогда $|T| = 2^{r-1} \lfloor \log_2 k \rfloor > \frac{n}{4} \lfloor \log_2 k \rfloor$.

Теперь пусть $2^r + r - 1 < n < 2^{r+1} + r, r \in \mathbb{N}$. Последнее по номеру из K_i будет иметь как минимум 2^{r-1} наборов. Также заметим, что $\log_2 n < \log_2(2^{r+1} + r) \leq r + 2$. Тогда получаем, что $r - 1 > \log_2 n - 3$. Отсюда следует, что $|T| \geq 2^{r-1} \lfloor \log_2 k \rfloor > \frac{n}{8} \lfloor \log_2 k \rfloor$.

При $k \neq 2$ и $k \neq 3$

$$|T| \geq \frac{n}{8}\lfloor \log_2 k \rfloor \geq \frac{n}{8}(\log_2 k - 1) = \frac{n}{8}\log_2 \frac{k}{2} \geq \frac{n}{8}\log_2 \sqrt{k} = \frac{n}{16}\log_2 k.$$

При $k = 2$ и при $k = 3$ положим

$$|T| \geq \frac{n}{8}.$$

Список литературы

[1] 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, 197–200.

[2] Романов Д. С., “О тестах относительно перестановок переменных в булевых функциях”, *Прикладная математика и информатика*, 2012, № 41, М.: МАКС Пресс, 113–121.

On checking tests with respect to local permutations of circuit inputs

Lopunov M. A.

The paper establishes the order of growth of the Shannon function of the length of the checking test relative to the source of faults, which can arbitrarily swap any k of consecutive inputs of the circuit.

Key words: checking test, tests on circuit inputs, Shannon function, permutations.

References

[1] Glazunov N.I., Goryashko A. P., “Estimates of the lengths of detecting tests for classes of non-constant faults in the inputs of combinational circuits”, *Izv. AN SSSR. Ser. «Technicheskaya kibernetika»*, 1986, № 3, 197–200 (In Russian).

[2] Romanov, D.S., “Tests with respect to permutations of variables in Boolean functions”, *Computational Mathtmatics and Modeling*, **24** (2013), 558–565.