А. А. Вороненко, Д. В. Чистиков

РАСШИФРОВКА БЕСПОВТОРНЫХ ФУНКЦИЙ ОРАКУЛОМ — СЧЕТЧИКОМ ЧЕТНОСТИ*

Задачи тестирования управляющих систем были впервые подробно описаны И. А. Чегис и С. В. Яблонским в работе [1] и с тех пор изучались для различных дискретных объектов. Тестовые постановки возникали, например, в теории дискретных функций [2] и в вычислительной теории обучения (computational learning theory) [3]. Из разнообразных форм наиболее известны задачи *диагностического* и *проверяющего тестирования* (см., например, [4]), имеющие дело с неизвестным, находящимся в черном ящике представителем некоторого известного множества объектов. Целью диагностики является определение, какой именно объект находится в черном ящике, цель проверки – подтверждение гипотезы о том, что в ящике находится заранее заданный конкретный объект. Достижение этих целей осуществляется посредством запросов к определяемым постановкой задачи *оракулам*. Если выбор очередного запроса может учитывать результаты предыдущих, тестирование называется *условным* (*тест* представляет собой алгоритм), в противном случае – *безусловным* (*тест* – последовательность запросов). Задачу построения условного диагностического теста называют также задачей *расшифровки*, или *точной идентификации*.

Для *бесповторных* булевых функций (выразимых формулами над некоторым базисом без повторений переменных) различные постановки задачи расшифровки изучаются уже более двадцати пяти лет. Наиболее известный ранний результат в этой области был получен Л. Валиантом в уже упомянутой классической работе [3] и затем улучшен Д. Англуин, Л. Хеллерштейн и М. Карпински в работе [5], где приводится алгоритм расшифровки бесповторных в *элементарном* базисе $B_0 = \{\&, \vee, \neg\}$ функций при помощи $O(n^3)$ запросов к оракулу, возвращающему значение неизвестной функции в точке (*точечных* запросов), и $O(n)$ запросов к оракулу, проверяющему совпадение неизвестной функции с функцией, задаваемой некоторой бесповторной формулой (ответ «да» в случае совпадения, иначе – контрпример входного набора; Валиант в своей работе использовал еще один оракул в дополнение к этим двум). В последней работе описывается также алгоритм расшифровки бесповторных в базисе $\{\&, \vee\}$ функций, использующий только $O(n^2)$ точечных запросов. В рабо-

* Работа выполнена при финансовой поддержке РФФИ (проекты 09-01-00701 и 09-01-00817)

те [6] решается задача расшифровки бесповторных функций в базисе всех симметрических функций и всех функций k переменных для произвольного натурального k: предлагаемый авторами алгоритм использует полиномиальное число запросов к двум описанным выше оракулам.

Ранее в работе [7] была поставлена задача *тестирования относительно бесповторной альтернативы*, заключающаяся в построении для бесповторной функции, существенно зависящей от всех своих переменных, проверяющего теста на множестве всех бесповторных функций тех же переменных (разрешается использовать лишь точечные запросы). Для базиса всех функций двух переменных было показано, что *функция Шеннона* длины теста (наибольшее из необходимых для тестирования функций n переменных количеств наборов) имеет квадратичный порядок роста (точное значение было впоследствии установлено Л. В. Рябцом [8]). Предлагаемый в работе метод квадратов существенности был в дальнейшем обобщен [9] на случай базиса всех функций l переменных для произвольного $l \geq 2$, а соответствующие оценки $\Theta(n^l)$ функции Шеннона сложности тестирования доказаны для случаев $l = 3, 4$. Доказательству для случая $l = 5$ посвящена работа [10]. В работе [11] доказываются линейные верхняя и нижняя оценки функции Шеннона длины теста в элементарном базисе. Универсальная нижняя оценка $\Omega(\sqrt{n})$ для сложности тестирования в базисе $\{\&, \vee\}$ доказывается в работе [12]; там же построен пример индивидуальной верхней того же порядка с близкой константой, а также улучшающие универсальную оценку индивидуальные нижние для функций, выразимых ДНФ и КНФ.

В настоящей работе рассматривается следующая задача. Для заданного базиса B требуется построить условный диагностический тест на множестве всех бесповторных в B функций, существенно зависящих от n переменных. Используется оракул – счетчик четности, возвращающий сумму по модулю два всех значений функции на произвольном запрашиваемом подкубе произвольной размерности. Возможностью быстрого нахождения правильных ответов на запросы соответствующего типа располагает, например, вычислитель, имеющий в своем распоряжении представление находящейся в черном ящике функции в виде полинома Жегалкина. Соответствующий алгоритм требует времени, линейного относительно длины полинома, так как сумма по модулю два всех значений булевой функции переменных $x_1, \ldots, x_k$ совпадает с коэффициентом ее полинома при слагаемом $x_1 \ldots x_k$.

Определим для каждого базиса B минимальную *длину теста* $T_B^{\oplus}(n)$ – количество запросов к оракулу в худшем случае. Целью настоящей работы является получение квадратичной верхней оценки данной ве-

личины для элементарного базиса B_0 и экспоненциальной нижней – для базисов, допускающих бесповторное выражение всех функций из B_0 и содержащих не являющиеся бесповторными в B_0 функции. Все рассматриваемые базисы будем считать *наследственными*, то есть содержащими вместе с каждой функцией все ее подфункции. Отметим, что для оракула, возвращающего значение в точке, соответствующее значение в случае элементарного базиса $T_{B_0}(n) = 2^n - 1$, поскольку число единиц у всякой существенно зависящей от всех своих переменных бесповторной в B_0 функции нечетно (см., например, лемму 1 настоящей работы), а расшифровка неизвестной конъюнкции n литералов требует в худшем случае не менее $2^n - 1$ запроса.

Лемма 1. *Пусть $n \geq 1$, функция $f(x_1,\ldots,x_n)$ бесповторна в базисе B_0. Тогда число единиц f нечетно тогда и только тогда, когда все ее переменные существенны.*

Доказательство. Функция, имеющая хотя бы одну фиктивную переменную, не может иметь нечетное число единиц. Если же все переменные существенны, то f представима в виде конъюнкции или дизъюнкции бесповторных в B_0 функций непересекающихся множеств переменных, среди которых нет фиктивных. Количество единиц f, таким образом, есть произведение количеств единиц этих функций либо 2^n минус произведение количеств нулей. Функции x_i^σ имеют по одной единице, а произведение нечетных чисел всегда нечетно. Лемма доказана.

Нам понадобится еще одно определение. Будем называть *правильным* корневое дерево для бесповторной в элементарном базисе функции $f(x_1,\ldots,x_n)$, представляющее структуру бесповторной формулы для f с поднятыми отрицаниями и функциональными символами $\&$ и $\vee$ произвольной арности. Более строго, листья дерева должны быть помечены литералами различных переменных из $\{x_1,\ldots,x_n\}$, а внутренние вершины – символами $\&$ и $\vee$, причем смежные вершины не могут быть помечены одинаковыми символами. Доказательство единственности правильного дерева излагалось еще В. А. Гурвичем в работе [13] в 1977 году.

Лемма 2. *Пусть $n \geq 2$, функция $f(x_1,\ldots,x_n)$ бесповторна в базисе B_0 и существенно зависит от всех своих переменных. Пусть известна существенно зависящая от всех своих переменных функция $g(x_1,\ldots,x_{n-1})$ такая, что*

$$f(x_1,\ldots,x_{n-1},\alpha_n) \equiv g(x_1,\ldots,x_{n-1})$$

для известного $\alpha_n \in \{0,1\}$. Тогда можно построить $2n-3$ набора аргументов функции f, по значениям на которых эта функция восстанавли-

вается однозначно.

Доказательство. Не ограничивая общности рассуждений, будем считать функцию g (обратим внимание, что, вообще говоря, не f) монотонной по всем своим переменным. Пусть g имеет вид

$$g(x_1,\ldots,x_{n-1}) = \varphi(x_1 \circ \ldots \circ x_s, x_{s+1},\ldots,x_{n-1}),$$

где $s \geq 2$ и $\circ \in \{\&,\vee\}$. Пусть, к примеру, $\circ$ есть дизъюнкция (случай конъюнкции рассматривается аналогичным образом). Построим s наборов функции f, по значениям на которых можно установить, справедливо ли равенство

$$f(x_1,\ldots,x_n) = \psi(x_1 \vee \ldots \vee x_s, x_{s+1},\ldots,x_{n-1},x_n)$$

для хотя бы одной бесповторной в B_0 функции ψ, и, если это не так, найти истинное из равенств

$$f(x_1,\ldots,x_n) = \varphi((x_{i_1} \ldots \vee x_{i_r}) \cdot x_n^{\alpha_n} \vee x_{i_{r+1}} \ldots \vee x_{i_s}, x_{s+1},\ldots,x_{n-1}).$$

Рассмотрим наборы

$$(10\ldots0\,\gamma_{s+1}\ldots\gamma_{n-1}\,\overline{\alpha}_n)$$

$$(01\ldots0\,\gamma_{s+1}\ldots\gamma_{n-1}\,\overline{\alpha}_n)$$

$$\ldots$$

$$(00\ldots1\,\gamma_{s+1}\ldots\gamma_{n-1}\,\overline{\alpha}_n)$$

с такими константами $\gamma_{s+1},\ldots,\gamma_{n-1}$, что $\varphi(x,\gamma_{s+1},\ldots,\gamma_{n-1}) \equiv x$. В случае если существует функция ψ с описанными выше свойствами, значения f на всех перечисленных наборах совпадают. Если же это не так, то в правильном дереве f не все из листьев $x_1,\ldots,x_s$ смежны с общей родительской вершиной, помеченной дизъюнкцией, а потому f допускает представление, задаваемое выписанным выше равенством, для которого $\{i_1,\ldots,i_r\}$ – множество всех номеров i таких, что i-й выбранный набор обращает f в 0, причем $1 \leq r \leq s-1$. В этом случае восстановление функции f завершается.

Рассмотрим теперь подробнее первый случай. Сделаем замену переменных $y = x_1 \vee \ldots \vee x_s$ и перейдем к восстановлению функции ψ, существенно зависящей от $n-s+1$ переменной. Выбрав в ее правильном дереве внутреннюю вершину, потомками которой являются только листья, повторим предыдущие рассуждения. Либо ψ будет восстановлена по значениям на очередных построенных наборах (прообразы нуля и единицы для переменной y выбираются произвольно), либо окажется возможной еще одна замена переменных и процесс будет продолжен. Рассу-

ждения предыдущего абзаца оказываются неприменимыми только в случае функции $g \equiv x$, существенно зависящей ровно от одной переменной, но тогда возможны лишь случаи $f = x \,\&\, x_n^{\alpha_n}$ и $f = x \vee x_n^{\overline{\alpha}_n}$, различающиеся на любом наборе с $x_n = \overline{\alpha}_n$.

Рассчитаем количество наборов, достаточное для восстановления f в худшем случае. Описанная замена требует s наборов и уменьшает количество переменных восстанавливаемой функции на $s-1$. Если замена будет возможна вплоть до $g \equiv x$, то количество переменных g будет суммарно уменьшено на $n-2$, причем в худшем случае каждая из переменных потребует двух наборов. Следовательно, для восстановления f в любом случае достаточно $2 \cdot (n-2)+1 = 2n-3$ наборов, что и требовалось доказать.

Теорема 1. *Для элементарного базиса* $B_0 = \{\&, \vee, \neg\}$

$$T^{\oplus}_{B_0}(n) \le n^2 - n + 1.$$

Доказательство. Опишем алгоритм расшифровки неизвестной функции, бесповторной в элементарном базисе и существенно зависящей от всех своих переменных. Проведем доказательство по индукции. Функции x_1 и $\overline{x}_1$ можно различить при помощи любого точечного запроса. Рассмотрим переменную x_n функции $f(x_1,\ldots,x_n)$. Заметим, что подстановка одной из констант на ее место не изменяет существенности остальных. Действительно, пусть для определенности f монотонна по выбранной переменной, тогда подходящей константой является 0, если в правильном дереве x_n связана с дизъюнкцией, и 1 в противном случае (в случае антимонотонности обе константы инвертируются). С учетом леммы 1 это означает, что запрос суммы по модулю два значений f на подкубе $(-\ldots-\beta_n)$ для произвольно выбранного $\beta_n \in \{0,1\}$ позволяет выбрать подходящую константу как $\alpha_n = \beta_n$ в случае ответа 1 и $\alpha_n = \overline{\beta}_n$ в случае ответа 0. Перейдя к рассмотрению функции

$$g(x_1,\ldots,x_{n-1}) = f(x_1,\ldots,x_{n-1},\alpha_n),$$

проведем полную процедуру ее расшифровки. По предположению индукции (выполняемые запросы дополняются значениями $x_n = \alpha_n$) для этого достаточно $(n-1)^2-(n-1)+1$ запроса. Согласно лемме 2, для восстановления f по g достаточно выполнить $2n-3$ точечных запроса. Следовательно, полная расшифровка f требует не более

$$1 + ((n-1)^2 - (n-1) + 1) + (2n-3) = n^2 - n + 1$$

запроса, что и завершает доказательство теоремы.

Замечание. Из доказательства видно, что среди всех выполняемых

запросов только $n-1$ обращен к подкубам ненулевой размерности (остальные запросы – точечные). Ответы на эти запросы использовались нами лишь для того, чтобы определить наличие или отсутствие фиктивных переменных у той или иной подфункции находящейся в черном ящике функции. Отметим без доказательства, что если множество возможных функций в постановке задачи включает все бесповторные функции n переменных (не ограничивается функциями, все переменные которых существенны), то уже в случае элементарного базиса требуется не менее $(3/2)^n$ запросов к используемому нами оракулу [14].

Исследуем теперь сложность рассматриваемой задачи для базисов, отличных от элементарного. В. А. Стеценко [15] описал все функции, не являющиеся бесповторными в B_0, но обладающие только бесповторными в B_0 подфункциями (далее *функции Стеценко*, используется также термин «слабоповторные функции»). Это функции

$$
\begin{aligned}
f_t^{(s)} &= x_1 \ldots x_s \vee \bar{x}_1 \ldots \bar{x}_s, && s \geq 2,\\
f_m^{(s)} &= x_1(x_2 \vee \ldots \vee x_s) \vee x_2 \ldots x_s, && s \geq 3,\\
f_d^{(s)} &= x_1(x_2 \vee x_3 \ldots x_s) \vee x_2\bar{x}_3 \ldots \bar{x}_s, && s \geq 3,\\
f_4 &= x_1(x_2 \vee x_3) \vee x_3x_4,\\
f_5 &= x_1(x_3x_4 \vee x_5) \vee x_2(x_3 \vee x_4x_5),
\end{aligned}
$$

а также все функции, получаемые из перечисленных перестановками переменных и навешиванием отрицаний на какие-либо переменные и, возможно, на сами функции. Всякий наследственный базис, содержащий не являющуюся бесповторной в B_0 функцию, обязан содержать хотя бы одну функцию Стеценко. Назовем функцию *нулевой*, если нулей у нее не меньше, чем единиц.

Лемма 3. *Для любой нулевой функции Стеценко s переменных и запроса к подкубу размерности d вероятность получения ответа* 1 *равна* 0 *при* $d = s$ *и не превосходит* 1/2 *при* $d \leq s-2$ (*распределение на множестве запросов считается равномерным*).

Доказательство. Непосредственная проверка показывает, что всякая функция Стеценко имеет четное число единиц, так что в случае $d = s$ утверждение леммы справедливо. Рассмотрение только нулевых функций обеспечивает справедливость леммы для запросов нулевой размерности.

Табл. 1. Функции $f_t^{(s)}$, $s \geq 2$

Размерность запроса	Свободные переменные	Подкубы с нечетным числом единиц	Вероятность ответа 1
$1 \leq d \leq s-2$	$x_1,\ldots,x_d$	$(-\ldots-0\ldots0)$ $(-\ldots-1\ldots1)$	$2/2^l$

Табл. 2. Функции $f_m^{(s)}$, $s \geq 3$

Размерность запроса	Свободные переменные	Подкубы с нечетным числом единиц	Вероятность ответа 1
$2 \leq d \leq s-2$	$x_1,\ldots,x_d$	$(-\ldots-0\ldots0)$ $(-\ldots-1\ldots1)$	$2/2^l$
	$x_2,\ldots,x_{d+1}$	$(0-\ldots-1\ldots1)$ $(1-\ldots-0\ldots0)$	$2/2^l$
$d=1$	x_1	$(-\alpha_2\ldots\alpha_s)$, $(\alpha_2\ldots\alpha_s) \neq \mathbf{0},\mathbf{1}$	$1-2/2^{s-1}$
	x_2	$(0-1\ldots1)$ $(1-0\ldots0)$	$2/2^{s-1}$

Осталось изучить значения $1 \leq d \leq s-2$. Заметим, что все собственные подфункции функций Стеценко бесповторны в B_0, и воспользуемся леммой 1. Перечислим все подкубы с нечетным числом единиц (таблицы 1–5; символы **0** и **1** обозначают наборы (0…0) и (1…1) подходящей размерности) с учетом имеющихся симметрий: функции $f_t^{(s)}$, $f_m^{(s)}$ и $f_d^{(s)}$ переходят в себя под действием любых перестановок всех переменных, начиная с x_1, x_2 и x_3 соответственно, а функция f_5 не меняется при перестановке $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ номеров ее переменных. Вычислив для каждого множества из d переменных долю подкубов с нечетным числом единиц (удобно использовать обозначение $l = s-d$), убедимся в справедливости утверждения леммы.

Табл. 3. Функции $f_d^{(s)}, s \geq 3$

Размерность запроса	Свободные переменные	Подкубы с нечетным числом единиц	Вероятность ответа 1
$3 \leq d \leq s-2$	$x_1,\ldots,x_d$	$(-\ldots-0\ldots0)$ $(-\ldots-1\ldots1)$	$2/2^l$
$2 \leq d \leq s-2$	$x_1,x_3,\ldots,x_{d+1}$	$(-0-\ldots-1\ldots1)$ $(-1-\ldots-0\ldots0)$	$2/2^l$
	$x_2,\ldots,x_{d+1}$	$(0-\ldots-0\ldots0)$ $(1-\ldots-1\ldots1)$	$2/2^l$
	$x_3,\ldots,x_{d+2}$	$(01-\ldots-0\ldots0)$ $(10-\ldots-1\ldots1)$	$2/2^l$
$d=2$	x_1,x_2	$(--\alpha_3\ldots\alpha_s)$, $(\alpha_3\ldots\alpha_s) \neq \mathbf{0},\mathbf{1}$	$1-2/2^{s-2}$
$d=1$	x_1	$(-01\ldots1)$ $(-1\alpha_3\ldots\alpha_s)$, $(\alpha_3\ldots\alpha_s) \neq \mathbf{0}$	$1/2$
	x_2	$(0-0\ldots0)$ $(1-\alpha_3\ldots\alpha_s)$, $(\alpha_3\ldots\alpha_s) \neq \mathbf{1}$	$1/2$
	x_3	$(01-0\ldots0)$ $(10-1\ldots1)$	$2/2^{s-1}$

Во всех случаях, кроме двух (запросы размерности $d=1$ к функциям $f_m^{(s)}$, $s \geq 3$ и размерности $d=2$ к функциям $f_d^{(s)}$, $s \geq 4$), необходимая оценка получается без дополнительных вычислений; для указанных исключений достаточно применить смешанную цепочку

$$p\cdot(1-q)+(1-p)\cdot q=(1-2p)\cdot q+2p\cdot\frac{1}{2}\le\max\left\{q,\frac{1}{2}\right\}=\frac{1}{2}$$

с $(p,q)=(s^{-1},2^{-(s-2)})$ и $\left(\binom{s}{2}^{-1},2^{-(s-3)}\right)$ соответственно. Лемма доказана.

Табл. 4. Функция f_4

Размерность запроса	Свободные переменные	Подкубы с нечетным числом единиц	Вероятность ответа 1
$d=2$	x_1,x_2	$(--00)$ $(--01)$	1/2
	x_1,x_3	$(-0-0)$ $(-1-1)$	1/2
	x_1,x_4	$(-01-)$ $(-11-)$	1/2
	x_2,x_3	$(1--0)$ $(1--1)$	1/2
	x_2,x_4	нет	0
	x_3,x_4	$(00--)$ $(01--)$	1/2
$d=1$	x_1	(-100) (-101) (-110) (-010)	1/2
	x_2	$(1-00)$ $(1-01)$	1/4
	x_3	$(00-1)$ $(01-1)$ $(10-0)$ $(10-1)$	1/2
	x_4	$(001-)$ $(011-)$	1/4

Фиксируем теперь какие-нибудь $s\ge 2$ и $\beta\in[0;1)$. В дальнейшем мы положим s равным арности некоторой нулевой функции Стеценко и выберем значение $\beta=1/2$. Рассмотрим равномерное распределение на множестве $\binom{n}{l}$ двоичных наборов длины n, содержащих ровно l единиц. Пусть $n=ps+q$ и $0\le q<s$. Рассмотрим случайные величины $\xi_1,\xi_2,\ldots,\xi_p$, выражающиеся через соответствующие количества $l_1,l_2,\ldots,l_p$ единиц в первых, вторых, …, p-х s позициях по правилу

$$\xi_i = \begin{cases} 0 & \text{при } l_i = 0, \\ 1 & \text{при } l_i = 1, \\ \beta & \text{иначе.} \end{cases}$$

Положим теперь $\xi = \xi_1 \cdot \ldots \cdot \xi_p$. Обозначим символом $\mathsf{E}\xi$ математическое ожидание случайной величины ξ. Справедливо следующее утверждение:

Лемма 4. *Для любого* $s \geq 2$ *выполнено* $\max\limits_{l} \mathsf{E}\xi = 1/2^{\Omega(n)}$.

Доказательство. Рассмотрим сумму, выражающую значение $\mathsf{E}\xi$. Продемонстрируем, что для всякого $s \geq 2$ найдется такая положительная константа δ, что для всякой последовательности $l = l(p)$, заключенной между p и $(1+\delta)p$, доля ненулевых слагаемых в этой сумме убывает с ростом p не медленнее некоторой геометрической прогрессии. Из этого будет следовать утверждение леммы, ибо при $l < p$ всегда $\xi \equiv 0$, а при $l > (1+\delta)p$ непременно $\xi \leq \beta^{\Omega(p)} = 1/2^{\Omega(n)}$.

Рассмотрим произвольный набор, соответствующий ненулевому слагаемому. Выберем в каждой группе из s позиций с номерами $(i-1)s+1,\ldots,is$ $(1 \leq i \leq p)$ какую-нибудь единичную. Оставшиеся единичные позиции задают сочетание из $n-p$ элементов по $l-p$. Это означает, что доля ненулевых слагаемых в сумме не превосходит

$$\frac{s^p \cdot \binom{n-p}{l-p}}{\binom{n}{l}} = \frac{s^p \cdot (n-p)_{l-p} \cdot l!}{(l-p)! \cdot (n)_l} = \frac{s^p \cdot (l)_p}{(n)_p} \leq \frac{s^p \cdot (l)_p}{(sp)_p} = \prod_{k=0}^{p-1} \frac{s \cdot (l-k)}{sp-k}.$$

Выберем теперь какое-нибудь число $\omega \leq 1$ и определим, сколько сомножителей в последнем произведении не превосходят ω. Неравенство $s(l-k) \leq \omega(sp-k)$ выполняется при $k \geq k_\omega = s \cdot (l - \omega p)/(s-\omega)$, поэтому количество подходящих k равно $p - k_\omega$. Пусть теперь $0 < \omega < 1$. Число сомножителей, больших 1, равно k_1, причем все они не превосходят $sl/(s-1)p$.

Табл. 5. Функция f_5

Размерность запроса	Свободные переменные	Подкубы с нечетным числом единиц	Вероятность ответа 1
$d=3$	x_1,x_2,x_3	$(---01)$ $(---10)$	$1/2$
	x_1,x_2,x_4	$(--0-1)$ $(--1-0)$	$1/2$
	x_1,x_3,x_4	$(-0--0)$ $(-1--1)$	$1/2$
	x_2,x_3,x_4	$(0---1)$ $(1---0)$	$1/2$
	x_2,x_3,x_5	$(0--1-)$ $(1--0-)$	$1/2$
	x_3,x_4,x_5	$(01---)$ $(10---)$	$1/2$
$d=2$	x_1,x_2	$(--011)$ $(--110)$ $(--101)$ $(--111)$	$1/2$
	x_1,x_3	$(-0-10)$ $(-1-01)$	$1/4$
	x_1,x_4	$(-01-0)$ $(-10-1)$	$1/4$
	x_1,x_5	$(-000-)$ $(-001-)$ $(-010-)$ $(-100-)$	$1/2$
	x_3,x_4	$(01--1)$ $(10--0)$	$1/4$
	x_3,x_5	$(01-1-)$ $(10-1-)$ $(11-0-)$ $(11-1-)$	$1/2$
$d=1$	x_1	(-0110) (-0001) (-0111) (-1001)	$1/4$
	x_3	$(01-00)$ $(01-01)$ $(01-10)$ $(10-10)$ $(11-00)$ $(11-10)$	$3/8$
	x_4	$(010-1)$ $(101-0)$	$1/8$

Следовательно, все произведение оценивается сверху числом

$$\omega^{p-k_\omega}\cdot\left(\frac{sl}{(s-1)p}\right)^{k_1}=\omega^{\frac{p\cdot(s-\omega)-s\cdot(l-\omega p)}{s-\omega}}\cdot\left(\frac{s}{s-1}\cdot\frac{l}{p}\right)^{\frac{s}{s-1}\cdot(l-p)},$$

которое при $p\le l\le(1+\delta)p$ не превосходит

$$\omega^{\frac{\omega\cdot(s-1)-\delta\cdot s}{s-\omega}\cdot p}\cdot\left(\frac{s}{s-1}\cdot(1+\delta)\right)^{\frac{s}{s-1}\cdot\delta p}.$$

Последнее выражение представляет собой p-ю степень не зависящей от p функции, которая для всяких фиксированных s и ω стремится при $\delta \to 0$ к заключенному между нулем и единицей числу

Это означает, что всякое достаточно малое $\delta \le \delta_0(s,\omega)$ удовлетворяет нашим требованиям. Лемма доказана.

Базис B будем называть *сложным*, если он содержит хотя бы одну

$$\omega^{\frac{\omega \cdot (s-1)}{s-\omega}}.$$

нелинейную и хотя бы одну немонотонную функции, и *неэлементарным*, если не все его функции бесповторно выразимы в базисе $B_0 = \{\&, \vee, \neg\}$.

Теорема 2. *Для наследственного, сложного и неэлементарного базиса B*

$$T_B^{\oplus}(n) = 2^{\Omega(n)}.$$

Доказательство. Согласно результатам [15], всякий наследственный неэлементарный базис содержит функцию Стеценко φ, существенно зависящую от $s \ge 2$ переменных. Наследственный сложный базис обязан содержать отрицание, так что бесповторной в B является и некоторая нулевая функция Стеценко того же числа переменных. Рассмотрим вспомогательное множество A_n всех бесповторных конъюнкций p функций φ и q отдельных переменных. Пусть T – условный диагностический тест на множестве $A_n' = \left\{ f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) : f \in A_n, \sigma_1, \ldots, \sigma_n \in \{0,1\} \right\}$ (отметим, что все функции из A_n' бесповторны в B, так как всякий наследственный сложный базис допускает бесповторную формулу для конъюнкции двух переменных). В силу леммы 3 и леммы 4 с $\beta = 1/2$ любой запрос дает ответ 1 с вероятностью, не превышающей $\varepsilon_n = 1/2^{\Omega(n)}$. Вероятность получения последовательности из t ответов 0, таким образом, не меньше $1 - t\varepsilon_n$. Следовательно, для диагностики необходимо (вообще говоря) не менее $\varepsilon_n^{-1} \cdot (1 - 2|A_n'|^{-1}) = 2^{\Omega(n)}$ запросов. Теорема доказана.

Из теоремы 1 и теоремы 2 вытекает следующий критерий:

Теорема 3. *Задача построения условного диагностического теста на множестве всех бесповторных в сложном наследственном базисе B функций, существенно зависящих от n переменных, допускает решение полиномиальным относительно n числом запросов к оракулу — счетчику четности в том и только в том случае, когда все функции из B бесповторно выразимы в элементарном базисе $B_0 = \{\&, \vee, \neg\}$.*

Литература

1. *Чегис И. А., Яблонский С. В.* Логические способы контроля электрических схем // Тр. матем. ин-та им. В. А. Стеклова. **51**. 1958. С. 270–360.
2. *Hansel G.* Sur le nombre des fonctions bool´eennes monotones de n variables // C. R. Acad. Sci. Paris, 1966, **262**. P. 1088–1090. (Русский перевод: *Ансель Ж.* О числе монотонных булевых функций n переменных // Кибернетический сборник, изд-во Мир. Новая серия. Вып. 5, 1968. С. 53–57.)
3. *Valiant L. G.* A theory of the learnable // Communications of the ACM. **27**, 1984. P. 1134–1142.
4. *Яблонский С. В.* Некоторые вопросы надежности и контроля управляющих систем // Математические вопросы кибернетики. Вып. 1. М.: Наука. Физматлит, 1988. С. 5–25.
5. *Angluin D., Hellerstein L., Karpinski M.* Learning read-once functions with queries // Journal of the ACM. **40**, 1993. P. 185–210.
6. *Bshouty N. H., Hancock T. R., Hellerstein L.* Learning boolean read-once formulas over generalized bases // Journal of Computer and System Sciences. 50:3, 1995. P. 521–542.
7. *Вороненко А. А.* О проверяющих тестах для бесповторных функций // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 163–176.
8. *Рябец Л. В.* Сложность проверяющих тестов для бесповторных булевых функций // Серия: Дискретная математика и информатика. Вып 18. Иркутск: Изд-во Ирк. гос. пед. ун-та, 2007. 30 с.
9. *Вороненко А. А.* Распознавание бесповторности в произвольном базисе // Прикладная математика и информатика. 2006. **23**. С. 67–84.
10. *Вороненко А. А., Чистиков Д. В.* О тестировании бесповторных булевых функций в базисе B_5 // Материалы XVII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Новосибирск, 27 октября – 1 ноября 2008 г.). Новосибирск: Изд-во Института математики, 2008 г. С. 24–30.
11. *Вороненко А. А.* О длине проверяющего теста для бесповторных функций в базисе $\{0,1,\&,\vee,\neg\}$ // Дискретная математика. **17**. № 2. 2005. С. 139–143.

12. *Бубнов С. Е., Вороненко А. А., Чистиков Д. В.* Некоторые оценки длин тестов для бесповторных функций в базисе {&,∨} // Прикладная математика и информатика. 2009. **33**. С. 90–100.

13. *Гурвич В. А.* О бесповторных булевых функциях // Успехи математических наук. 1977. **32**. № 1. С. 183–184.

14. *Voronenko A. A.* New learning and testing problems for read-once functions // arXiv:0912.3627 [cs.CC]

15. *Стеценко В. А.* О предплохих базисах в P_2 // Математические вопросы кибернетики. Вып. 4. М.: Физматлит, 1992. С. 139–177.