А.А. Вороненко, Д.В. Кафтан

О ДЛИНЕ СЕРТИФИКАТА ПОВТОРНОСТИ В БАЗИСЕ ВСЕХ ФУНКЦИЙ l ПЕРЕМЕННЫХ

Данная работа посвящена задаче доказательства повторности булевых функций в базисе всех функций l переменных. В работе показано, что длина сертификата повторности функций в таком базисе ограничена полиномом степени, не превосходящей наибольшего числа переменных базисной функции. Функция называется *повторной* в базисе B, если она не представима в этом базисе формулой без повторения переменных. *Сертификатом повторности* булевой функции f в базисе B называется множество наборов значений переменных такое, что значения функции f на этих наборах доказывают её повторность в B. Рассматриваемый базис B_l – базис всех функций l переменных – является *наследственным*, то есть содержащим вместе с любой функцией все ее подфункции, полученные подстановкой констант на места переменных. Назовем функцию f - *бесповторной*, если она представима над B_l формулой без повторения переменных. Рассмотрим следующие преобразования:

1) перестановка переменных;
2) замена переменной на ее отрицание;
3) замена функции на ее отрицание.

Эти преобразования называются *преобразованиями обобщенной однотипности* [1]. Функции, которые могут быть получены друг из друга преобразованиями обобщенной однотипности, называются *обобщенно однотипными*. Заметим, что отношение обобщенной однотипности является отношением эквивалентности.

Функция называется *слабоповторной* в базисе B_l, если все ее подфункции, полученные подстановкой констант на места переменных, являются бесповторными в базисе B_l, в то время как сама функция является повторной. Функция называется *разложимой*, если она представима в виде бесповторной суперпозиции других функций в рассматриваемом базисе. В противном случае функция называется *неразложимой*. Константа σ называется *забивающей* для функции $f(y_1, \dots, y_n)$ по переменной y_i, если функция $f(y_1, \dots, y_{i-1}, \sigma, y_{i+1}, \dots, y_n)$ содержит фиктивные переменные. В противном случае константа σ называется *незабивающей*.

Бесповторные в базисе B_l функции представимы в виде помеченного ориентированного дерева следующего вида:

1) Каждый лист помечен переменной, и каждой переменной соответствует ровно один лист.
2) Если внутренняя вершина смежна с листом, то она может иметь степень захода один и быть помечена отрицанием.
3) Каждая внутренняя вершина дерева помечена неразложимой функцией из B_l арности не меньше трех или символом из множества $\{\vee, \&, \oplus\}$. Каждой дуге, входящей в вершину, сопоставлена одна из переменных функции этой вершины. Вершины, помеченные символами $\{\vee, \&, \oplus\}$, могут иметь произвольное количество входных дуг, не меньшее двух.
4) Смежные вершины не могут быть помечены одной и той же функцией из множества $\{\vee, \&, \oplus\}$.
5) Функция реализуется в корне дерева.

Данное представление единственно с точностью до преобразований обобщенной однотипности (см., напр., [2], [3]).

В работах [4,5] доказаны следующие утверждения:

Утверждение 1 ([5]). *Минимальный сертификат повторности функции в стандартном базисе* $B_0 = \{\vee, \&, \neg\}$ *содержит 4 набора для неполяризуемых функций и 6 наборов для поляризуемых функций.*

Утверждение 2 (теорема 10 и следствие 11 в работе [4]). *Минимальная длина сертификата повторности в базисе* B_2 *есть величина порядка* $\Theta(n)$ *и для доказательства повторности в базисе всех функций двух переменных достаточно предъявить не более* $3n + 1$ *наборов.*

Также в работе [4] доказано, что сертификат повторности функции в базисе $B^{(s)} = B_0 \cup \{h_t^{(s)}\}$, где $h_t^{(s)}$– слабоповторная в базисе функция вида $h_t^{(s)} = x_1 \dots x_s \vee \bar{x}_1 \dots \bar{x}_s$, содержит $\Omega(n^{s-1})$ наборов при $n \to \infty$. Так как при добавлении функций в базис длина сертификата повторности монотонно не убывает, то из этого следует:

Утверждение 3. *Минимальный сертификат повторности функции в базисе* B_l *содержит* $\Omega(n^{l-1})$ *наборов при* $n \to \infty$.

Сформулируем основную теорему настоящей работы.

Теорема. *Минимальный сертификат повторности функции в базисе* B_l *содержит* $O(n^l)$ *наборов при* $n \to \infty$.

Если бы были справедливы обобщения одного из двух следующих утверждений, то существовали бы короткие пути доказательства основной теоремы.

Утверждение 4 (теорема Субботовской [6]). Любая слабоповторная функция в базисе B_0 имеет переменную, для которой обе константы являются незабивающими.

Соответствующим гипотетическим утверждением является следующее:

Гипотеза 1. Любая слабоповторная функция в базисе B_l имеет переменную, для которой обе константы являются незабивающими.

Утверждение 5 (теорема Стеценко [7]). Из любой повторной в базисе B_0 функции можно подстановкой констант получить подфункцию, обобщенно-однотипную с одной из функций Стеценко:

1) $f_d^{(s)} = x_1(x_2 \vee x_3 \cdot \ldots \cdot x_s) \vee x_2\bar{x}_3 \cdot \ldots \cdot \bar{x}_s$, $s \geq 3$;
2) $f_t^{(s)} = x_1 \cdot \ldots \cdot x_s \vee \bar{x}_1 \cdot \ldots \cdot \bar{x}_s$, $s \geq 2$;
3) $f_m^{(s)} = x_1(x_2 \vee \ldots \vee x_s) \vee x_2 \cdot \ldots \cdot x_s$, $s \geq 3$;
4) $f_4 = x_1(x_2 \vee x_3) \vee x_3x_4$;
5) $f_5 = x_1(x_2 \vee x_3 \cdot x_4) \vee x_5(x_3 \vee x_2 \cdot x_4)$.

Гипотеза 2. Для любого l существует такое число $r(l)$, что любая слабоповторная в B_l функция не менее чем $r(l)$ переменных принадлежит одному из трех семейств Стеценко $f_d^{(s)}$, $f_t^{(s)}$ и $f_m^{(s)}$.

Для доказательства теоремы нам потребуется несколько вспомогательных утверждений.

Лемма 1. Пусть функция $g(y_1, \ldots, y_m, x)$ бесповторна в B_l. Пусть $g(y_1, \ldots, y_m, \sigma) = y_1 \vee \ldots \vee y_m$. Пусть g имеет вид $\varphi_0 \vee f(\varphi_1, \ldots, \varphi_k, x)$, где φ_i – дизъюнкции различных переменных. Тогда g однозначно восстанавливается по значениям на $\binom{m}{k} \cdot 2^k$ наборах.

Доказательство. Функция g при $x = \sigma$ имеет вид $g(y_1, \ldots, y_m) = y_1 \vee \ldots \vee y_m$. Для восстановления g достаточно определить, в какую дизъюнкцию φ_i входит каждая переменная y_j. Выберем произвольно k переменных. Без ограничения общности рассуждений, пусть это будут первые k переменных $y_1, \ldots, y_k$. Заменим все переменные, кроме выбранных переменных и x, на ноль. Так как ноль является незабивающей константой для любой переменной в дизъюнкции, то все остальные переменные останутся существенными. Таким образом, если $y_1, \ldots, y_k$ входят, соответственно, в $\varphi_1, \ldots, \varphi_k$, то останется подфункция вида $f(y_1, \ldots, y_k, x)$, которая однозначно определяется по значениям на 2^k наборах с $x = \bar{\sigma}$, так как известна ее подфункция при $x = \sigma$. Если среди переменных $y_1, \ldots, y_k$ най-

дутся две переменные y_{j_1} и y_{j_2}, входящие в одну дизъюнкцию, например φ_1, то полученная функция будет иметь вид $h(y_{j_1} \vee y_{j_2}, y_{j_3}, \dots, y_{j_k}, x)$, где h – некоторая булева функция k переменных. Если хотя бы одна переменная y_i входит в функцию φ_0, то полученная функция будет иметь вид $y_i \vee h(y_{j_1}, \dots, y_{j_{k-1}}, x)$. Иначе переменные $y_1, \dots, y_k$ входят в разные дизъюнкции $\varphi_1, \dots, \varphi_k$, и полученная функция будет с точностью до перестановки переменных равна $f(y_1, \dots, y_k, x)$. Таким образом, мы найдем функцию f и множество переменных $y_1, \dots, y_k$, входящих в разные дизъюнкции.

Переберем все возможные множества из k переменных. Это можно сделать $\binom{m}{k}$ способами. Таким образом, мы найдем все переменные, от которых зависят $\varphi_1, \dots, \varphi_k$ и не зависит φ_0. Покажем, какие из них входят в одну и ту же дизъюнкцию. Рассмотрим пару y_1 и y_2. Если они входят в разные дизъюнкции φ_i и φ_j, то встретилась хотя бы одно множество из k переменных, с помощью которых согласно вышеуказанной процедуре получается функция f. Таким образом, функции $f(\varphi_1, \dots, \varphi_k, x)$ и φ_0 определяются с точностью до перестановки переменных и функция g полностью восстанавливается по значениям на $\binom{m}{k} \cdot 2^k$ наборах. Лемма доказана.

Лемма 2. Пусть функция $g(y_1, \dots, y_m, x)$ бесповторна в B_l. Пусть $g(y_1, \dots, y_m, \sigma) = y_1 \& \dots \& y_m$. Пусть g имеет вид $\varphi_0 \& f(\varphi_1, \dots, \varphi_k, x)$, где φ_i – конъюнкции различных переменных. Тогда g однозначно восстанавливается по значениям на $\binom{m}{k} \cdot 2^k$ наборах.

Доказательство. Проводится аналогично лемме 1, с той лишь разницей, что для любой переменной конъюнкции незабивающей константой является единица. Изменив соответствующим образом константные подстановки, получим те же самые $\binom{m}{k} \cdot 2^k$ наборов. Лемма доказана.

Лемма 3. Пусть функция $g(y_1, \dots, y_m, x)$ бесповторна в B_l. Пусть $g(y_1, \dots, y_m, \sigma) = y_1 \oplus \dots \oplus y_m$. Пусть g имеет вид $\varphi_0 \oplus f(\varphi_1, \dots, \varphi_k, x)$, где φ_i – суммы по модулю два различных переменных. Тогда g однозначно восстанавливается по значениям на $\binom{m}{k} \cdot 2^k$ наборах.

Доказательство. Проводится аналогично лемме 1. Так как обе константы являются незабивающими для любой переменной в сумме по модулю два, то можно заменить константные подстановки на любые, учитывая тот факт, что подстановка с нечетным числом единиц добавляет отрицание над суммой по модулю два. Лемма доказана.

Допустим, что количество переменных базисной функции f не известно заранее. Любое множество наборов для случая $k < l-1$ входит в некоторое множество наборов для случая $k = l-1$, так как каждый подкуб меньшей размерности k входит в подкуб большей размерности $l-1$, а константные подстановки на места остальных переменных не зависят от функции f. По виду функций, полученных для каждого множества из l функций, k определяется как максимальное число переменных функции вида $h(y_{j_1}, \dots, y_{j_k}, x)$, где $y_{j_1}, \dots, y_{j_k}$ не входят в φ_0 и входят в разные φ_i. Таким образом, верно следующее:

Следствие. Функция g, удовлетворяющая условиям леммы 1, 2 или 3, однозначно восстанавливается по $\binom{m}{l-1} \cdot 2^{l-1}$ наборам.

Лемма 4. Пусть дано помеченное корневое ориентированное дерево D. Тогда число корневых поддеревьев с корнем в некоторой вершине v и не более чем p вершинами, такими, что любая внутренняя вершина входит в поддерево вместе со всеми смежными в D вершинами, не превосходит 4^{p-1}.

Доказательство. Рассмотрим произвольную планарную реализацию дерева D и произвольное поддерево D' с корнем в вершине v. Закодируем D' следующим образом: если в дереве $p-k$ вершин, запишем в начале кода $2k$ нулей. Далее, обходя D' по правилу левой руки, будем записывать 1, если переходим по входящей дуге, и 0 – если по исходящей. Таким образом, первая встреченная в коде единица будет означать начало обхода. Каждая дуга встретится дважды и будет соответствовать: нулю при выходе из вершины и единице при входе. Покажем, что такое кодирование однозначно задает это поддерево в дереве D. Начнем обход дерева D из вершины v по правилу левой руки согласно коду дерева D'. Заметим, что любая вершина, которая встретилась во время обхода, либо входит в дерево D' со всеми своими входами в дереве D, либо является листом. Этого достаточно, чтобы, находясь в некоторой вершине, знать, продолжается ли обход в глубину и по какой входящей дуге дерева D, или что осуществляется возврат по исходящей дуге. Таким образом, поддерево D' можно однозначно выделить в дереве D. Количество таких деревьев не больше, чем число кодирующих наборов. Для дерева с $p-k$ вершинами и, соответственно, $p-k-1$ дугами длина кода равна $2p-2k-2+2k = 2p-2$, а число двоичных наборов длины $2p-2$ равно 2^{2p-2}. Таким образом, число корневых поддеревьев с корнем в вершине v и не более чем p, вершинами не превосходит 4^{p-1}. Лемма доказана.

В работе [8] показано, что справедливо следующее утверждение:

Утверждение 6 (Следствие из теоремы Чистикова [8]). Проверяющий тест для бесповторной в базисе B_l функции, существенно зависящей от n переменных, на множестве всех -бесповторных функций содержит не более $\binom{n}{l} \cdot 2^l$ наборов.

Доказательство основной теоремы. Пусть функция f повторна в базисе B_l. Тогда у нее существует слабоповторная подфункция $g(x_1, \dots, x_m)$. Известно (см. [9]), что у любой булевой функции есть переменная, для которой существует незабивающая константа. Тогда у g найдутся переменная x_i и константа σ такие, что подфункция g', полученная подстановкой σ на место x_i, существенно зависит от всех остальных переменных. Полученная подфункция будет -бесповторна. По утверждению 6, она однозначно задается на $\binom{m-1}{l} \cdot 2^l$ наборах.

Рассмотрим дерево D, реализующее произвольную бесповторную функцию от переменных $x_1, \dots, x_m$, совпадающую с $g(x_1, \dots, x_m)$ при $x_i = \sigma$. При подстановке $x_i = \sigma$ из этого дерева получается поддерево D', реализующее -бесповторную функцию g'. Это могло произойти следующим образом:

1) Некоторое поддерево D'' дерева D' соответствует функции, полученной подстановкой $x_i = \sigma$ в функцию f' из B_l, которой помечена некоторая вершина в дереве D. Выделим такое поддерево. Пусть это поддерево имеет корень в вершине v. В нем не более чем $l - 1$ листьев, соответствующих входам вершины, помеченной f' в дереве D. Подставим константы на места переменных так, чтобы каждая функция, соответствующая входу функции f', равнялась какой-либо переменной, а функция, которую реализует дерево D, равнялась функции f'. Получим подкуб размерности l, половина которого при $x_i = \sigma$ нам уже известна. Таким образом, на 2^{l-1} наборах целиком определяется функция f', и, следовательно, восстанавливается функция, которую реализует дерево D. Функция g либо отличается на каком-то из этих наборов от функции, которую реализует дерево D для любой такой функции f', либо совпадает с ней на этих наборах, но отличается на каком-то еще наборе. Таким образом, достаточно предъявить $2^{l-1} + 1$ набор, чтобы отличить g от любой бесповторной функции с подфункцией f', чья подфункция при $x_i = \sigma$ представляет собой поддерево D''. Посчитаем количество поддеревьев, которые можно выделить таким образом. С помощью индукции легко доказывается, что число вершин степени не меньше двух в дереве меньше количества листьев. Поэтому в D' не более $2l - 2$ вер-

шин. Поддерево D' удовлетворяет условию леммы 4, и количество таких поддеревьев не превосходит 4^{2l-3}. Таким образом, чтобы отличить g, соответствующие таким деревьям, достаточно не более $m \cdot (2^{l-1}+1) \cdot 4^{2l-3}$ наборов.

2) Переменная x_i в дереве D смежна с вершиной, помеченной функцией от двух переменных, которая отождествляется со второй переменной или ее отрицанием при подстановке $x_i = \sigma$. Функций, соответствующих дереву D в этом случае, не более 3 на каждое ребро. Так как все вершины, кроме листовых и смежных с ними, имеют степень не меньше двух, то общее число вершин в дереве не больше $3m$. Таким образом, чтобы отличить все функции, устроенные таким образом, достаточно не более $3 \cdot 3m$ наборов.
3) Переменная x_i в дереве D входит в вершину v_1, помеченную неразложимой функцией из B_l, которая при подстановке $x_i = \sigma$ превращается в функцию из множества $\{\vee, \&, \oplus\}$ и входит в вершину v_2, помеченную той же функцией. Подставим константы на места переменных таким образом, чтобы на каждом входе этих двух вершин была одна переменная. Полученная функция удовлетворяет условию леммы 1, 2 или 3. Рассмотрим наборы, полученные в соответствующей лемме. Если функция, реализуемая деревом D, совпадает с g на всех $\binom{m-1}{k-1} \cdot 2^{k-1}$ наборах, то у нее существует хотя бы один другой набор, в котором она отличается от g. Если не совпадает, то повторность доказывается предъявлением всех использованных наборов. Для разных бесповторных функций, полученных из этой вершины, предъявленные наборы будут одинаковыми, так как одинаковы функции на входах функций в вершинах v_1 и v_2. Таким образом, согласно следствию из вспомогательных лемм, повторность g в этом случае доказывается предъявлением не более чем $\binom{m-1}{l-1} \cdot 2^{l-1} + 1$ набора для каждой такой вершины и в целом не более $m \cdot \binom{m-1}{l-1} \cdot 2^{l-1} + m = O(m^l)$ наборов для всей функции.

Всего суммарно получается $3 \cdot 3m + m \cdot (2^{l-1}+1) \cdot 4^{2l-3} + m \cdot \binom{m-1}{l-1} \cdot 2^{l-1} + m = O(m^l)$ наборов, которых достаточно, чтобы отличить функцию $g(x_1, \dots, x_m)$ от всех бесповторных, совпадающих с ней при $x_i = \sigma$. Так как $m \le n$, то для доказательства повторности функции f достаточно предъявить $O(n^l) + \binom{n-1}{l-1} \cdot 2^l = O(n^l)$ наборов значений переменных. Теорема доказана.

Литература

1. Перязев Н. А. Слабоповторные булевы функции в бинарном базисе// Дискретная математика и информатика. Вып. 4. Иркутск: Изд-во Иркут. ун-та, 1998. 12 с.
2. Кузнецов А. В. О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики. Труды МИАН СССР. Т. 51. 1958. С. 186–225.
3. Вороненко А. А. Распознавание бесповторности в произвольном базисе. Прикладная математика и информатика. Вып. 23. 2006. С. 67–84.
4. Chistikov D., Fedorova V., Voronenko A. Certificates of Non-Membership for Classes of Read-Once Functions. TUCS Lecture Notes No. 17, pp. 48–53 (2012).
5. Вороненко А. А., Федорова В. С., Чистиков Д. В. Повторность булевых функций в элементарном базисе // Известия вузов. Математика. – 2011. – Т. 55. – №. 11. – С. 11-61.
6. Субботовская Б.А. О сравнении базисов при реализации функций алгебры логики формулами, ДАН СССР 149 (4), 784–787 (1963).
7. Стеценко В. А. О предплохих базисах в P2 // Матем. вопросы кибернетики. Вып. 4. М.: Физматлит, 1992. С. 139–177
8. Chistikov D. V. Checking Tests for Read-Once Functions over Arbitrary Bases //Computer Science–Theory and Applications. – Springer Berlin Heidelberg, 2012. – С.52-63.
9. Лупанов О. Б. О сложности реализации функций алгебры логики формулами //Проблемы кибернетики. – 1960. – Т. 3. – С. 61-80.