



УДК 519.11, 519.71

О доле неповторных функций, свободных от лап большой ширины

О. В. Зубков

Восточно-Сибирская государственная академия образования

Аннотация. В статье сравниваются мощности некоторых классов булевых функций, неповторных в полном бинарном базисе $B_2 = \{\&, \vee, \oplus\}$. Неповторные функции представляются помеченными корневыми деревьями, среди которых выделяются канонические. Далее приводится алгоритм, позволяющий переходить от канонических деревьев к полным бинарным каноническим деревьям. Данный алгоритм связывает два принципиально различных подхода к построению однозначного представителя для неповторной в B_2 функции. Представление неповторных функций в виде полных бинарных канонических деревьев позволяет доказать, что среди всех неповторных функций от n переменных, доля функций, в каноническом представлении которых содержится хотя бы одна k -местная функция $\&$, $\vee$ или $\oplus$ экспоненциально стремится к нулю с ростом величины k . Данный результат представляет интерес для тестирования неповторных функций.

Ключевые слова: неповторные булевы функции; полный бинарный базис; каноническое представление неповторной функции; помеченное корневое дерево; полное бинарное каноническое дерево; тестирование булевых функций относительно неповторной альтернативы.

1. Два вида канонических представлений в виде дерева для неповторной в B_2 булевой функции и связь между ними

Формула Φ над базисом B называется неповторной, если каждая переменная входит в нее не более одного раза. Булева функция f называется неповторной в базисе B , если найдется неповторная формула Φ над B , представляющая функцию f . Далее в работе под базисом будем понимать полный бинарный базис $B_2 = \{\&, \vee, \oplus, -\}$.

Корневое дерево называется бинарным, если каждая его вершина имеет не более двух потомков, причем про каждого известно, является ли он левым или правым. Если при этом каждая вершина либо имеет двух потомков, либо не имеет ни одного, такое бинарное дерево назы-

вается полным. Вершину, являющуюся правым (левым) потомком, но не являющуюся листом, будем называть правым (левым) узлом.

Рассмотрим следующую каноническую форму представления бесповторных в B_2 булевых функций в виде помеченного корневого полного бинарного дерева.

Определение 1. Упорядоченным термом над B_2 от переменных $x_1, x_2, \dots, x_n$ будем называть бесповторный терм Φ , удовлетворяющий следующим требованиям:

- (1) в терме Φ отрицания могут быть только над переменными;
- (2) для любого подтерма $\Phi_1 * \Phi_2$ терма Φ , где $*$ $\in \{\&, \vee, \oplus\}$, переменная с наименьшим индексом среди всех переменных подтерма $\Phi_1 * \Phi_2$ содержится в подтерме Φ_1 ;
- (3) в терме Φ не содержится подтермов вида $(\Phi_1 \& \Phi_2) \& \Phi_3$, $(\Phi_1 \vee \Phi_2) \vee \Phi_3$, $(\Phi_1 \oplus \Phi_2) \oplus \Phi_3$;
- (4) для любого подтерма $\Phi_1 \oplus \Phi_2$ терма Φ переменная с наименьшим индексом среди переменных подтерма Φ_2 входит в Φ_2 без отрицания.

В [2] доказано, что для любой бесповторной в B_2 функции существует единственный упорядоченный терм, представляющий ее.

Определение 2. По упорядоченному терму Φ построим помеченное корневое полное бинарное дерево G . Каждому литералу $x_i^{\sigma_i}$ терма Φ соответствует лист дерева G с пометкой $x_i^{\sigma_i}$. Каждому подтерму $\Phi_1 * \Phi_2$ терма Φ , где $*$ $\in \{\&, \vee, \oplus\}$, соответствует внутренняя вершина T дерева G , помеченная $*$. Левый потомок вершины T соответствует Φ_1 , правый потомок соответствует Φ_2 . Корень дерева G соответствует всему терму Φ .

Далее будем использовать указанное взаимно однозначное соответствие вершин дерева G и подтермов терма Φ для упрощения изложения. Получившееся помеченное корневое полное бинарное дерево будем называть бинарным каноническим деревом. Из того факта, что по бесповторной в B_2 функции однозначно строится упорядоченный над B_2 терм, а по нему взаимно однозначно строится бинарное каноническое дерево следует, что для каждой бесповторной в B_2 функции существует единственное бинарное каноническое дерево.

Из пункта (3) определения упорядоченного терма следует, что в бинарном каноническом дереве пометки двух смежных внутренних вершин могут совпадать только в том случае, когда одна из них является правым потомком другой.

Каждому подтерму $\Phi_1 * \Phi_2$ можно взаимно однозначно поставить в соответствие наименьшую по индексу переменную терма Φ_2 , которую назовем правой ключевой переменной для подтерма $\Phi_1 * \Phi_2$ и соответствующей ему вершины дерева G . То, что по вершине можно од-

позначно указать его правую ключевую переменную очевидно по определению последней. В обратную сторону однозначность показывается следующим образом. Пусть x_i является правой ключевой переменной по крайней мере для одной вершины. Если x_i является наименьшей по индексу в двух разных поддермах, то один из них является поддермом (левым потомком) другого. Отсюда единственным образом найдется максимальный по включению подтерм Φ_2 , для которого x_i является наименьшей по индексу. Так как x_i правая ключевая, то Φ_2 входит в подтерм вида $\Phi_1 * \Phi_2$, для которого она и является правой ключевой. Φ_2 является правым потомком.

В [1] рассмотрен другой способ построения по неповторной в B_2 булевой функции канонического представления, которое названо каноническим деревом.

Определение 3. Каноническим деревом назовем помеченное корневое дерево, удовлетворяющее следующим условиям:

1. Константой (0 или 1) может быть помечена лишь вершина, являющаяся единственной в дереве.
2. Листья дерева помечены переменными или их отрицаниями (литералами). Разные листья помечены литералами, соответствующими различным переменным.
3. Внутренние вершины помечены либо линейными ($\oplus, \oplus$), либо нелинейными ($\&, \vee$) символами.
4. Смежные вершины помечены различными символами. Смежные вершины не могут быть помечены линейными символами.
5. Вершина, лежащая над помеченой линейным символом и смежная с ней не может быть помечена $\&$ или отрицанием переменной.

Далее приведем алгоритм перехода от канонического дерева к бинарному каноническому дереву. Вершину канонического дерева, имеющую k потомков, будем называть лапой ширины k .

Алгоритм 1.

- 1) Все лапы ширины $k \geq 2$ привести к упорядоченному виду $*(\Phi_1, \dots, \Phi_k)$, так что Φ_1 содержит наименьшую по индексу переменную всей лапы, Φ_2 содержит наименьшую по индексу среди всех переменных лапы, не входящих в $\Phi_1, \dots, \Phi_{k-1}$ содержит наименьшую среди переменных из Φ_{k-1} и Φ_k .
- 2) Все лапы ширины $k \geq 3$ вида $*(\Phi_1, \dots, \Phi_k)$, где $*$ это многоместная базисная функция из множества $\{\&, \vee, \oplus\}$, представить в виде $*(\Phi_1, *(\Phi_2, \dots, *(\Phi_{k-1}, \Phi_k) \dots))$. Если $*$ = $\oplus$, то в дереве перейти к ветке вида $\oplus(\Phi_1, \oplus(\Phi_2, \dots, \oplus(\Phi_{k-1}, \Phi_k) \dots))$.
- 3) Используя следующую процедуру, добиться правильной расстановки отрицаний над линейными символами и над их правыми ключевыми переменными (отрицания над этими элементами должны отсутствовать). Пусть Φ – первая вершина, помеченная линейным символом,

на пути из некоторого листа в корень дерева, в которой каким-либо образом нарушена расстановка отрицаний.

- Если Φ это $\Phi_1 \oplus \Phi_2$ и над наименьшей по индексу переменной в Φ_2 (правой ключевой для $\Phi_1 \oplus \Phi_2$) стоит отрицание, то воспользоваться эквивалентностью $\Phi_1 \oplus \Phi_2 = \bar{\Phi}_1 \oplus \bar{\Phi}_2$.

- Если Φ это $\Phi_1 \bar{\oplus} \Phi_2$ и над его правой ключевой переменной нет отрицания, то воспользоваться эквивалентностью $\Phi_1 \bar{\oplus} \Phi_2 = \bar{\Phi}_1 \oplus \Phi_2$.

- Если Φ это $\Phi_1 \bar{\oplus} \Phi_2$ и над его правой ключевой переменной стоит отрицание, то воспользоваться эквивалентностью $\Phi_1 \bar{\oplus} \Phi_2 = \Phi_1 \oplus \bar{\Phi}_2$.

Далее, пользуясь законами де Моргана и преобразованием $\Psi_1 \bar{\oplus} \Psi_2 = \bar{\Psi}_1 \oplus \Psi_2$ установить отрицания над переменными. Использование эквивалентности $\Psi_1 \bar{\oplus} \Psi_2 = \bar{\Psi}_1 \oplus \Psi_2$ гарантирует, что если до преобразования для текущей вершины условие (4) упорядоченности не нарушалось, то оно не нарушится и после преобразования.

Повторять шаг 3) алгоритма до тех пор, пока расстановка отрицаний где-либо нарушена.

Пример 1. На рис. 1 приведено каноническое дерево для функции

$$(\bar{x}_1 \vee (x_{10} \bar{\oplus} x_{11})) \oplus (\bar{x}_2 \vee x_7) \oplus (\bar{x}_3 \& \bar{x}_5 \& x_6 \& \bar{x}_8 \vee \bar{x}_4 \vee x_9).$$

На рис. 2 приведено бинарное каноническое дерево для той же самой функции. Дерево соответствует упорядоченному терму

$$(\bar{x}_1 \vee (\bar{x}_{10} \oplus x_{11})) \oplus ((x_2 \& \bar{x}_7) \oplus ((x_3 \vee (x_5 \vee (\bar{x}_6 \vee x_8))) \& (x_4 \& \bar{x}_9))).$$

Правые узлы отмечены темным, левые узлы отмечены светлым. Правые ключевые переменные для правых узлов, упорядоченных слева направо снизу вверх: $x_{11}, x_3, x_4, x_6, x_8, x_9$.

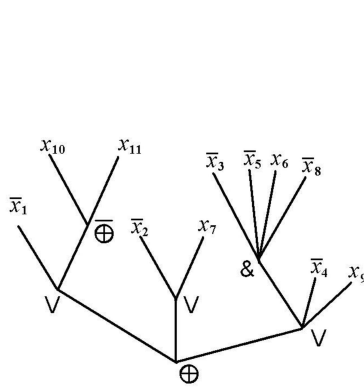


Рис. 1.

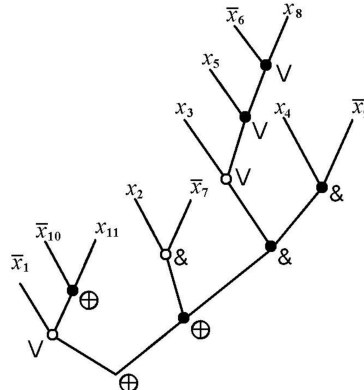


Рис. 2.

2. Построение шаблона бинарного канонического дерева

Последовательность вершин $U_1, U_2, \dots, U_h$, в которой вершина U_1 произвольная, а для всех $2 \leq i \leq h$ вершина U_i является правым потомком вершины U_{i-1} , будем называть правым интервалом длины h . Если при этом интервал нельзя увеличить, то есть вершина U_1 является левым узлом или корнем дерева, а правый потомок вершины U_h является листом, такой правый интервал будем называть полным. Любой левый узел, либо корень является началом ровно одного полного правого интервала.

Так как лапа ширины k состоит из одинаковых бинарных функций, то, согласно условию (3) определения упорядоченности над B_2 , соответствующий ей правый интервал содержит $k - 2$ правых узлов. Отсюда следует, что если в бинарном каноническом дереве содержится менее чем $k - 2$ правых узлов, то соответствующая ему функция свободна от лап ширины k .

Пусть $k - 2 \leq d < n$ и G – бинарное каноническое дерево с n листьями и d правыми узлами. Для этого дерева определим следующим образом множество бинарных канонических деревьев $V(G)$, структура которых близка структуре дерева G . В дереве G удалим пометки всех правых узлов, а так же удалим отрицания (если они есть) над всеми правыми ключевыми переменными этих правых узлов. Полученное частично помеченное дерево назовем шаблоном дерева G . Если в нем произвольным образом расставить пометки непомеченных правых узлов символами бинарных базисных функций, а так же расставить произвольным образом отрицания над правыми ключевыми переменными этих узлов, получим некоторое помеченное дерево, соответствующее рассматриваемому шаблону. Для того, чтобы вновь полученное дерево было бинарным каноническим, при доопределении шаблона необходимо выполнение следующих требований:

- а) если левый потомок непомеченного узла U помечен символом $\&$, то узел U можно пометить либо символом $\vee$, либо символом $\oplus$;
- б) если левый потомок непомеченного узла U помечен символом $\vee$, то узел U можно пометить либо символом $\&$, либо символом $\oplus$;
- в) если левый потомок непомеченного узла U помечен символом $\oplus$, то узел U можно пометить либо символом $\&$, либо символом $\vee$;
- г) если левый потомок непомеченного узла U является листом, то узел U можно пометить любым из трех бинарных базисных символов;
- д) если узел U помечаем $\oplus$, то над его правой ключевой переменной отрицание не ставится;
- е) если узел U помечаем $\&$ или $\vee$ то над его правой ключевой переменной отрицание можно либо ставить, либо не ставить.

Все получаемые таким образом бинарные канонические деревья образуют множество $V(G)$. Они попарно различны. Исходное дерево G содержится в $V(G)$.

Следует отметить, что расстановка пометок в шаблоне может производиться в любом порядке. Уже установленные пометки никак не влияют на еще не установленные. Это позволяет подсчитать мощность множества $V(G)$.

Лемма 1. *Если шаблон бинарного канонического дерева G содержит d непомеченных правых узлов, среди которых m имеют левых потомков, помеченных $\&$ или $\vee$, p имеют левых потомков, помеченных $\oplus$, s имеют в качестве левых потомков листья, то число различных бинарных канонических деревьев, содержащихся в $V(G)$ равно $3^m \cdot 4^p \cdot 5^s$.*

Доказательство. Если левый потомок непомеченного узла U помечен символом $\oplus$, то существует четыре способа доопределения узла U , а именно:

- U пометить символом $\&$, его правую ключевую переменную оставить без отрицания,
- U пометить символом $\&$, над его правой ключевой переменной поставить отрицание,
- U пометить символом $\vee$, его правую ключевую переменную оставить без отрицания,
- U пометить символом $\vee$, над его правой ключевой переменной поставить отрицание.

Если левый потомок непомеченного узла U помечен символом $\&$ (символом $\vee$), то существует три способа доопределения узла U , а именно:

- U пометить символом $\vee$ ($\&$), его правую ключевую переменную оставить без отрицания,
- U пометить символом $\vee$ ($\&$), над его правой ключевой переменной поставить отрицание,
- U пометить символом $\oplus$, его правую ключевую переменную оставить без отрицания,

Аналогично можно установить, что если непомеченный узел U имеет в качестве левого потомка лист, то U можно доопределить всеми пятью способами.

В силу независимости доопределения узлов, получим, что верно утверждение леммы 1. $\square$

Пример 2. На рис. 3 приведен шаблон бинарного канонического дерева из примера 1. Для каждого непомеченного правого узла указано число способов его доопределения. Всего существует 5625 ($3^2 \cdot 5^4$) различных бинарных канонических деревьев, соответствующих данному

шаблону. Дерево состоит из четырех полных правых интервалов длины которых равны 4, 2, 1, 3.

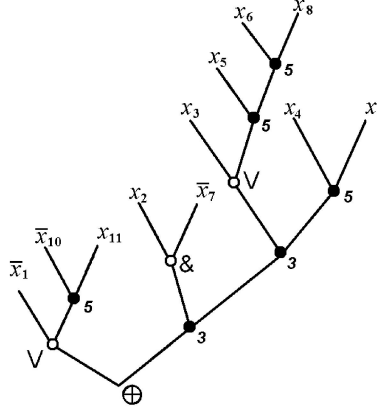


Рис. 3

3. О доле неповторных функций, свободных от лап ширины k

Теорема 1. Доля неповторных функций, свободных от лап ширины большей либо равной k , не меньше чем

$$1 - \frac{27n}{(3/2)^k}.$$

Доказательство. Оценим сверху число бинарных канонических деревьев, содержащихся в множестве $V(G)$ и содержащих хотя бы одну лапу ширины большей либо равной k . Множество таких деревьев обозначим через $I(G, k)$.

Лапа L ширины k состоит из $k - 1$ подряд расположенных одинаково помеченных узлов $T_1, \dots, T_{k-1}$, образующих правый интервал длины $k - 1$. Этот интервал входит в состав полного правого интервала $U_1, \dots, U_h$, где $k - 1 \leq h$. При этом вершины T_1 и U_1 могут совпадать, в этом случае в интервале $U_1, \dots, U_h$ требуется для создания лапы L пометить одинаковыми символами $k - 2$ подряд идущих узлов $U_2, \dots, U_{k-1}$. Если начала интервалов не совпадают, то в интервале $U_1, \dots, U_h$ требуется для создания лапы L пометить одинаковыми символами $k - 1$ подряд идущих узлов $U_i, \dots, U_{i+k-2}$.

Пусть Ω – количество всех способов выбора в шаблоне дерева G одного правого интервала длины $k - 1$ для создания лапы L . (Например, для шаблона, представленного на рис. 3, при $k - 1 = 2$, Ω равно 6.) Так как

при выборе конкретного места расположения лапы L начальная вершина T_1 совпадает с одной из вершин дерева, то заведомо выполняется неравенство $\Omega \leq n - 1$, где n – число листьев.

Далее для построения и оценки мощности множества деревьев, заведомо содержащего множество $I(G, k)$:

- выбранные $k - 1$ (либо $k - 2$) узлов помечаем одним и тем же символом бинарной функции (не более трех способов);
- над правыми ключевыми переменными этих $k - 1$ (либо $k - 2$) узлов произвольным образом расставим отрицания (не более чем 2^{k-1} способов).

Оставшиеся непомяченными не более чем $d - k + 2$ узлов, пометим всеми разрешенными в требованиях а) – е) способами. Пусть при этом для i -го способа выбора расположения лапы L ($1 \leq i \leq \Omega$), среди оставшихся непомяченными не более чем $d - k + 2$ узлов содержатся

- m_i узлов, левые потомки которых помечены символами $\&$ или $\vee$;
- p_i узлов, левые потомки которых помечены символом $\oplus$;
- s_i узлов, левые потомки которых являются листьями.

При переборе всех указанных параметров, получим не более чем

$$3 \cdot 2^{k-1} \cdot \sum_{i=1}^{\Omega} 3^{m_i} \cdot 4^{p_i} \cdot 5^{s_i} \text{ различных деревьев, соответствующих исходному}$$

шаблону. Среди них не все могут быть бинарными каноническими, но заведомо содержатся все бинарные канонические из $I(G, k)$, содержащие хотя бы одну лапу ширины большей либо равной k . Некоторые из элементов $I(G, k)$ могут встретиться более одного раза.

Далее считаем, что шаблон дерева G удовлетворяет условиям леммы 1. При этом, в зависимости от соотношения величин m, p, s и $k - 2$:

$$\max_{i=1}^{\Omega} (3^{m_i} \cdot 4^{p_i} \cdot 5^{s_i}) \leq \begin{cases} 3^{m-(k-2)} \cdot 4^p \cdot 5^s & \text{если } k - 2 \leq m; \\ 4^{p-p'} \cdot 5^s, & \text{если } m \leq k - 2 \leq m + p; \\ 5^{s-s'}, & \text{если } m + p \leq k - 2 \leq m + p + s = d; \end{cases}$$

где $p - p' = m + p - (k - 2)$, $s - s' = m + p + s - (k - 2)$.

Учитывая, что $\Omega < n$, получим в каждом из соответствующих случаев следующую оценку :

$$|I(G, k)| \leq 3 \cdot 2^{k-1} \cdot \sum_{i=1}^{\Omega} 3^{m_i} \cdot 4^{p_i} \cdot 5^{s_i} \leq \begin{cases} 3n \cdot 2^{k-1} \cdot 3^{m-(k-2)} \cdot 4^p \cdot 5^s \\ 3n \cdot 2^{k-1} \cdot 4^{p-p'} \cdot 5^s \\ 3n \cdot 2^{k-1} \cdot 5^{s-s'}. \end{cases}$$

Вычитая полученную верхнюю оценку множества $I(G, k)$ из числа всех бинарных канонических деревьев, содержащихся в множестве $V(G)$, получим нижнюю оценку числа бинарных канонических деревьев, свободных от лап ширины большей либо равной k . Мощность множества $V(G)$ находится по лемме 1 и равна $3^m \cdot 4^p \cdot 5^s$.

Поделив эту нижнюю оценку на $|V(G)|$, для каждого случая получим нижнюю оценку доли бинарных канонических деревьев, свободных от лап ширины большей либо равной k среди всех элементов множества $V(G)$:

$$\frac{|V(G)| - |I(G, k)|}{|V(G)|} \geq \begin{cases} 1 - \frac{3n \cdot 2^{k-1}}{3^{k-2}} \\ 1 - \frac{3n \cdot 2^{k-1}}{3^m \cdot 4^{p'}} \\ 1 - \frac{3n \cdot 2^{k-1}}{3^m \cdot 4^p \cdot 5^{s'}}. \end{cases}$$

Усилим оценку, во втором и третьем случаях заменив $4^{p'}$ на $3^{p'}$, 4^p на 3^p , $5^{s'}$ на $3^{s'}$. Учитывая, что $m + p' = k - 2$ и $m + p + s' = k - 2$, получим общую для всех трех случаев оценку

$$\frac{|V(G)| - |I(G, k)|}{|V(G)|} \geq 1 - \frac{9n}{(3/2)^{k-1}}.$$

Учитывая, что

- среди бинарных канонических деревьев, содержащих менее чем $k - 2$ правых узлов, доля деревьев, свободных от лап ширины большей либо равной k составляет 1;
 - бинарные канонические деревья, соответствующие разным шаблонам различны;
 - каждой бесповторной в B_2 бесповторной функции взаимно однозначно ставится в соответствие ее бинарное каноническое дерево,
- получим утверждение теоремы. □

Список литературы

1. Вороненко А. А. О проверяющих тестах для бесповторных функций // Математические вопросы кибернетики. — 2002. — вып. 11. — С. 163-176.
2. Зубков О. В. О числе бесповторных булевых функций в базисе $\{\&, \vee, \oplus, -\}$, Дискретный анализ и исследование операций. — 2003. — серия 1, Т. 10, N 1. — С. 41 - 60.

O. V. Zubkov

About a part noniterated functions, free from paws of the big width

Abstract. In this paper we are comparing noniterated in the whole binar basis $B_2 = \{\&, \vee, \oplus\}$ some classes powers of Boolean functions. Noniterated Boolean functions

are presented with a marked root trees, in which we can pick out the a canonical forms. To continue there is an algorithm, with the help of whitch we can pass from the canonical trees to the whole binar canonical trees. In this algorithm we can combine two definitely different methods of creating the canonical form of the noniterated in the basis B_2 function. The representation of the noniterated Boolean functions as a whole binar canonical trees allowed to proof, that the part of functions in canonical form of which there is one or more k-locative function $\&$, $\vee$ or $\oplus$ exponently aspires to zero with a growth of k-value. The result is worth testing of the noniterated Boolean function.

Keywords: noniterated Boolean function, whole binar basis, canonical forms of the noniterated function, marked root trees, whole binar canonical trees, testing of the Boolean functions concerning the noniterated alternative

Зубков Олег Владимирович, кандидат физико-математических наук, доцент, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Нижняя Набережная, 6 тел.: (3952)551138 (oleg.zubkov@mail.ru)

Zubkov Oleg, East Siberian State Education Academy, 6, N. Naberezhnaya St., Irkutsk, 664011, associate professor, Phone: (3952)551138 (oleg.zubkov@mail.ru)