Math-Net.Ru

Общероссийский математический портал

Н. А. Соловьев, Проверяющие тесты для суперпозиций булевых функций от элементарных однородных функций, *Дискрет. матем.*, 1996, том 8, выпуск 2, 117–132

DOI: <https://doi.org/10.4213/dm523>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.205.19.152

26 апреля 2023 г., 17:00:59

Проверяющие тесты для суперпозиций булевых функций от элементарных однородных функций

© 1996 г. Н. А. Соловьев

Рассматривается функция Шеннона, характеризующая длину минимального проверяющего теста, для суперпозиций булевых функций от элементарных однородных функций (константа, отрицание, конъюнкция, дизъюнкция, сложение по модулю 2). Выявляется класс исходных логических функций, на суперпозициях которых указанная функция Шеннона достигается. На основе изучения свойств таблиц различимости предложен общий подход к решению подобных задач.

1. Постановка задачи

Пусть $f(\tilde{x}_n)$, $\tilde{x}_n = (x_1, \dots, x_n)$, есть некоторая функция алгебры логики. Говорят, что функция $f(x_1, \dots, x_i, \dots, x_n)$ существенно зависит от переменной x_i , если

$$f(x_1, \dots, 0, \dots, x_n) \neq f(x_1, \dots, 1, \dots, x_n).$$

Предполагая существенную зависимость функции $f(\tilde{x}_n)$ от n переменных, рассмотрим множества

$$\mathfrak{X} = \{\mathfrak{X}_1, \dots, \mathfrak{X}_q\},$$

где $\mathfrak{X}_i = \{X_1^{(i)}, \dots, X_u^{(i)}\}$, $X_k^{(i)} \subseteq \tilde{x}_n$, $k = 1, \dots, q$, $i = 1, \dots, u$, $X_k^{(i)} \cap X_l^{(i)} = \emptyset$, если $k \neq l$,

$$\Phi_i = \{\varphi_1^{(i)}, \dots, \varphi_u^{(i)}\},$$

где $\varphi_k^{(i)}$ — функция алгебры логики от некоторых переменных из набора $\tilde{x}_n$, $k = 1, \dots, u$, $i = 1, \dots, q$.

Обозначим $F_i = F_i(f, \mathfrak{X}, \Phi)$ функцию, полученную из функции $f(\tilde{x}_n)$ путем подстановок вида $x \rightarrow \varphi_k^{(i)}$, если $x \in X_k^{(i)}$, и тождественных подстановок $x \rightarrow x$, если $x \in \tilde{x}_n \setminus \mathfrak{X}_i$.

Пусть $\mathfrak{F}$ есть некоторое множество функций F_i , полученных из функции $f(\tilde{x}_n)$ указанной выше операцией суперпозиции. Будем обозначать E_2^n множество всех бинарных наборов длины n и $\oplus$ операцию сложения по модулю 2.

Определение 1. Множество $\tau(f, \mathfrak{F})$ наборов $\tilde{\alpha}_n$ из E_2^n называется проверяющим тестом функции $f(\tilde{x}_n)$ относительно множества $\mathfrak{F}$, если для любой функции $F_i \in \mathfrak{F}$ найдется $\alpha_n \in \tau(f, \mathfrak{F})$ такое, что

$$\partial(f(\tilde{\alpha}_n), \mathfrak{x}_i, \Phi_i) = f(\tilde{\alpha}_n) \oplus F_i(f(\tilde{\alpha}_n), \mathfrak{x}_i, \Phi_i) \neq 0.$$

Определение 2. Таблицей различимости $D(f(\tilde{x}_n), \mathfrak{F})$ для функции $f(\tilde{x}_n)$ относительно множества $\mathfrak{F}$ называется таблица, строки которой суть наборы значений функции

$$\partial(f(\tilde{x}_n), \mathfrak{x}_i, \Phi_i) = f(\tilde{x}_n) \oplus F_i(f(\tilde{x}_n), \mathfrak{x}_i, \Phi_i).$$

Легко видеть, что таблица различимости $D(f(\tilde{x}_n), \mathfrak{F})$ является бинарной таблицей с $|E_2^n| = 2^n$ столбцами и числом строк, равным мощности множества $\mathfrak{F}$. Для определенности будем предполагать, что элементы множества E_2^n упорядочены в лексикографическом порядке.

Из определений 1 и 2 следует, что любое покрытие (единиц строк столбцами) таблицы различимости $D(f(\tilde{x}_n), \mathfrak{F})$ является проверяющим тестом функции $f(\tilde{x}_n)$ относительно множества $\mathfrak{F}$.

Рассмотрим функцию

$$\mathcal{L}(n, \mathfrak{F}) = \max_f \min_{\tau(f, \mathfrak{F}) \in \hat{\tau}(f, \mathfrak{F})} |\tau(f, \mathfrak{F})|, \quad (1)$$

где минимум берется по множеству $\hat{\tau}(f, \mathfrak{F})$ всех проверяющих тестов функции f относительно $\mathfrak{F}$, а максимум по множеству всех функций алгебры логики f , существенно зависящих от n переменных.

Задача заключается в оценке величины $\mathcal{L}(n, \mathfrak{F})$.

В настоящей работе исследуется случай, когда класс функций Φ является классом однородных элементарных функций, а именно, когда функции $\varphi = \varphi_k^{(i)}$ являются функциями только одного из следующих пяти типов: $\varphi = c$, $c \in \{0, 1\}$, $\varphi = \bar{x}$ (иначе $\varphi = x \oplus 1$, отрицание), $\varphi = x \& y$ (конъюнкция), $\varphi = x \vee y$ (дизъюнкция), $\varphi = x \oplus y$ (сложение по модулю 2).

Величину $q = |\mathfrak{X}|$ назовем кратностью суперпозиции, суперпозиция называется l -местной, если $l = \max_k |X_k^{(i)}|$.

Заметим, что полученные в настоящей работе результаты для суперпозиций единичной кратности справедливы и для суперпозиций произвольной кратности. Поскольку в данной работе рассматриваются только суперпозиции из элементарных однотипных функций, то в дальнейшем вместо общего символа $\mathcal{L}(n, \mathfrak{F})$ будем использовать символ $\mathcal{L}(n, o)$, где значок o служит обозначением логической операции, с помощью которой образуются функции φ_k .

Хотя в цитируемых выше работах [1–3] употребляется чисто техническая терминология (ошибка, неисправность, склейка и т. п.), в которых функция $f(\tilde{x}_n)$ заменяется логической моделью (схемой), способной ошибаться лишь на входах, там фактически исследуется множество функций, полученных из $f(\tilde{x}_n)$ операцией суперпозиции (либо единичной кратности, либо произвольной кратности) из функций φ_k одного и того же вида, а именно, функций $\varphi_k = c_k$, $c_k \in E_2 = \{0, 1\}$ [1, 2], $c_k \in E_g = \{0, 1, 2, \dots, g\}$, $g \geq 2$ [3], $\varphi_k = \bar{x}_k$ [3], либо из функций, отвечающих неисправностям, называемым склейкой (слипанием) входов схемы, моделирующей рассматриваемую функцию $f(\tilde{x}_n)$ [3]. Если некоторое

подмножество входов слипается, то через каждый из слипшихся входов проходит максимальный (по значению) сигнал из всех сигналов, поступающих на слипшиеся входы, другими словами, дизъюнкция сигналов. Склейка возможна при коротком замыкании проводов, обеспечивающих проводимость входов схемы.

Константные неисправности (при $\varphi_k = c_k$, $c_k \in E_g$) определяются тем, что существует непустое подмножество Y , $Y \subseteq \tilde{x}_n$, для которого

$$\varphi_k = \begin{cases} c_k, & \text{если } x_k \in Y, c_k \in E_g, \\ x_k, & \text{если } x_k \in \tilde{x}_n \setminus Y, \end{cases} \quad (2)$$

и являются частным случаем сдвигов

$$\varphi_k = \begin{cases} x_k \oplus_g c_k, & \text{если } x_k \in Y, \\ x_k, & \text{если } x_k \in \tilde{x}_n \setminus Y. \end{cases} \quad (3)$$

Здесь символ $\oplus_g$ означает операцию сложения по модулю g , при $g = 2$ значок 2 будем опускать.

При $g = 2$ сдвиги можно назвать инверсиями, они, как уже отмечалось, рассматриваются в работе [3]. Это название обусловлено тем, что выражение $x \oplus 1$ меняет значение x на обратное.

Определение 3. Функция $f(\tilde{x}_n)$ называется тестируемой относительно множества $\mathfrak{F}$, если для любой строки $\tilde{d}$ таблицы различимости $D(f(\tilde{x}_n), \mathfrak{F})$

$$\partial(f(\tilde{x}_n), \mathfrak{X}_i, \Phi_i) \neq 0,$$

где $\partial(f(\tilde{x}_n), \mathfrak{X}_i, \Phi_i)$ — функция, определяющая строку $\tilde{d}$.

Заметим, что если функция $f(\tilde{x}_n)$ тестируема относительно множества $\mathfrak{F}$, то по определению 3, соответствующая таблица различимости $D(f(\tilde{x}_n), \mathfrak{F})$ не имеет нулевых строк, а потому всегда существует покрытие множества единиц строк столбцами, т. е. всегда существует проверяющий тест.

Определение 4. Множество N строк $\tilde{d} = (d^{(1)}, d^{(2)}, \dots, d^{(2^n)})$ таблицы различимости $D(f(\tilde{x}_n), \mathfrak{F})$ называется ортогональным, если для любой пары строк $(\tilde{d}_i, \tilde{d}_j)$ из N имеют место соотношения $d_i^{(\lambda)} d_j^{(\lambda)} = 0$ для всех $\lambda \in \{1, 2, 3, \dots, 2^n\}$. Ортогональное множество N называется максимальным, если любое расширение N перестает быть ортогональным множеством, и наибольшим, если не существует никакого ортогонального множества N' такого, что $|N'| > |N|$.

Если при некотором $\lambda \in \{1, 2, 3, \dots, 2^n\}$ для пары строк $(\tilde{d}_i, \tilde{d}_j)$ таблицы различимости $D(f(\tilde{x}_n), \mathfrak{F})$ имеет место соотношение $d_i^{(\lambda)} d_j^{(\lambda)} = 1$, то говорят, что эта пара строк пересекается по единицам.

Пара функций (f_1, f_2) , определенных на множестве E_2^n , называется ортогональной, если при всех $\tilde{\alpha} \in E_2^n$ выполняется соотношение $f_1(\tilde{\alpha}) f_2(\tilde{\alpha}) = 0$.

Пример. Пусть задана функция $f(\tilde{x}_3) = x_1 + x_1 x_2 + x_1 x_3$, а функции φ определяются с помощью операции $\circ = \neg$ (инверсия). Здесь вместо знака $\oplus$ используется знак $+$. Поскольку рассматриваются только суперпозиции кратности 1, а

операция инверсии $\neg$ является одноместной, возможные варианты множеств $\mathfrak{X}_i$ суть $\{x_1\}$, $\{x_2\}$ и $\{x_3\}$. Положим для определенности, что $\mathfrak{X}_1 = \{x_1\}$, $\mathfrak{X}_2 = \{x_2\}$, $\mathfrak{X}_3 = \{x_3\}$, тогда $\varphi_1 = \neg x_1 = \bar{x}_1 = x_1 + 1$, $\varphi_2 = x_2 + 1$, $\varphi_3 = x_3 + 1$, а таблица различимости определяется функциями

$$F_1 = f(x_1, x_2, x_3) + f(\bar{x}_1, x_2, x_3) = x_3 + 1,$$

$$F_2 = f(\tilde{x}_3) + f(x_1, \bar{x}_2, x_3) = x_3,$$

$$F_3 = f(\tilde{x}_3) + f(x_1, x_2, \bar{x}_3) = x_1 + x_2.$$

Следовательно, таблица различимости $D(f(\tilde{x}_3), \mathfrak{F})$ имеет вид

$$D(f(\tilde{x}_3), \mathfrak{F}) = \left\| \begin{array}{cccccccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array} \right\|.$$

2. Тесты для инверсий

Соотношение (3) для инверсий ($g = 2$) можно описать набором

$$\tilde{c}_n = (c_1, c_2, \dots, c_n) \neq \tilde{0}_n$$

(для $\tilde{0}_n$ используем другое обозначение $(0)_n$), если каждой переменной x_i из множества Y поставить в соответствие константу $c_i = 1$, а остальным переменным (из множества $\tilde{x}_n \setminus Y$) — константу 0. Следуя [3], набор $\tilde{c}_n$ будем называть ошибкой. Напомним, что в дальнейшем будут рассматриваться только единичные ошибки $\tilde{e}^{(i)} = (0)_{i-1}(1)_1(0)_{n-i}$, $1 \leq i \leq n$.

Разлагая функцию $f(\tilde{x}_n) + f(\tilde{x}_n + \tilde{e}^{(i)})$, где

$$\tilde{x}_n + \tilde{e}^{(i)} = (x_1, x_2, \dots, x_{i-1}, x_i + 1, x_{i+1}, \dots, x_n)$$

по переменной x_i , получаем, что

$$f(\tilde{x}_n) + f(\tilde{x}_n + \tilde{e}^{(i)}) = x_i(f_{x_i}^1 + f_{x_i}^0) + (x_i + 1)(f_{x_i}^0 + f_{x_i}^1) = f_{x_i}^0 + f_{x_i}^1, \quad (4)$$

где $f_{x_i}^\sigma$ — функция, полученная из функции $f(\tilde{x}_n)$ замещением (подстановкой) переменной x_i константой σ .

Введем ради удобства для таблиц различимости обозначение $D(f(\tilde{x}_n), \circ)$, где символ $\circ$ служит обозначением операции, с помощью которой строятся функции подстановок φ_k , а следовательно, и множество функций $\mathfrak{F}$, а для строк таблиц различимости обозначение $\partial_X^2 f(\tilde{x}_n)$, $X = \{x\}$ или $X = \{x', x''\}$, означающее, что над элементами множества X производится одноместная или двухместная операция $\circ$.

Следовательно, согласно (4) таблица различимости $D(f(\tilde{x}_n), \neg)$ имеет вид

$$D(f(\tilde{x}_n), \neg) = \|\tilde{f}(\tilde{x}_n) + \tilde{f}(\tilde{x}_n + \tilde{e}^{(i)})\| = \|\tilde{f}_{x_i}^0 + f_{x_i}^1\|, \quad i = 1, \dots, n,$$

где $\tilde{g}(\tilde{x}_n)$ — вектор значений функции $g(\tilde{x}_n)$ на упорядоченном (в лексикографическом порядке) множестве E_2^n .

О переменной x_i , связанной со строкой

$$\partial_{x_i}^- f(\tilde{x}_n) = \tilde{f}(\tilde{x}_n) + \tilde{f}(\tilde{x}_n + \tilde{e}^{(i)}) = \tilde{f}_{x_i}^0 + \tilde{f}_{x_i}^1$$

(обозначим последнюю через $\tilde{d}_x$), будем говорить как о переменной, порождающей строку $\tilde{d}_x$ таблицы различимости $D(f(\tilde{x}_n), \neg)$.

Если переменная x является существенной переменной функции $f(\tilde{x}_n)$, то по определению $f_x^0 \neq f_x^1$. Тогда, обозначая через $\mathfrak{S}_-^{(1)}$ множество всех одиночных суперпозиций функций $\neg x_1, \neg x_2, \dots, \neg x_n$ от функции $f(\tilde{x}_n)$, из соотношения (4) получаем следующее утверждение.

Утверждение 1. *Любая функция алгебры логики $f(\tilde{x}_n)$, существенно зависящая от всех переменных $x_1, x_2, \dots, x_n$, является тестируемой функцией относительно множества $\mathfrak{S}_-^{(1)}$.*

Пусть $f(\tilde{x}_n)$ есть некоторая функция алгебры логики, существенно зависящая от n переменных.

Функция $f(\tilde{x}_n)$ называется линейно разделимой относительно множества $X \subseteq \tilde{x}_n$, если она представима в виде

$$f(\tilde{x}_n) = \sum_{x \in X} x \varphi_x + \varphi, \quad (5)$$

где сложение проводится по модулю 2 и множество $\bigcup_{x \in X} \{\varphi_x\}$ является множеством попарно ортогональных функций, причем каждая из функций φ_x и функция φ не зависят существенно от переменных из множества X . Число $q = |X|$ называется глубиной линейной разделимости функции $f(\tilde{x}_n)$.

Обозначим $t(n)$ наименьшее целое значение t , удовлетворяющее неравенству $n - t \leq 2^t$. Легко видеть, что указанная величина $t(n)$ однозначно определяется неравенствами $2^{t-1} + t \leq n \leq 2^t + t$.

Утверждение 2. *Наибольшее значение q глубины линейной разделимости функции $f(\tilde{x}_n)$, существенно зависящей от t переменных, равно $n - t(n)$.*

Доказательство. Пусть в соотношении (5) для функции $f(\tilde{x}_n)$ функция φ и функции φ_x в совокупности зависят от n переменных. Рассмотрим представление этих функций нормальными полиномами (т.е. полиномами в базисе $\{\&, +, \neg\}$) с конъюнкциями ранга t . Очевидно, мы получим максимальное число функций φ_x , если каждая из указанных функций φ_x будет представлена только одной конъюнкцией. Ясно, что число таких одиночных конъюнкций не более 2^t . Так как в представлении (5) каждой функции φ_x приписывается в качестве множителя только одна переменная из дополнительного (по отношению к множеству из t переменных) множества, множество всех n переменных рассматриваемой линейно разделимой функции должно удовлетворять неравенству $n - t \leq 2^t$. Очевидно, наибольшее значение величины получаем при минимальном значении t , удовлетворяющем указанному выше неравенству.

Утверждение 3. *Необходимым и достаточным условием ортогональности пары строк $(\tilde{d}_x, \tilde{d}_y)$ таблицы различимости $D(f(\tilde{x}_n), \neg)$ некоторой функции $f(\tilde{x}_n)$ является линейная разделимость функции $f(\tilde{x}_n)$ относительно множества $\{x, y\}$.*

Доказательство. Докажем необходимость. Пусть пара строк $(\tilde{d}_x, \tilde{d}_y)$ является парой ортогональных строк. Тогда по определению пара функций

$$(\partial_x^- f(\tilde{x}_n), \partial_y^- f(\tilde{x}_n)) = (f_x^0 + f_x^1, f_y^0 + f_y^1)$$

является парой ортогональных функций. Рассматривая полином Жегалкина (полином в базисе $\{\&, +\}$) для функции $f(\tilde{x}_n)$, воспользуемся следующим его преобразованием:

$$f(\tilde{x}_n) = xy\varphi_{xy} + x\varphi_x + y\varphi_y + \varphi.$$

Тогда

$$\partial_x^- f(\tilde{x}_n) = y\varphi_{xy} + \varphi_x, \quad \partial_y^- f(\tilde{x}_n) = x\varphi_{xy} + \varphi_y.$$

Необходимо показать, что $\varphi_{xy} \equiv 0$. Будем рассуждать от противного. Пусть $\varphi_{xy} \not\equiv 0$. Это означает существование набора $\tilde{\alpha}$, для которого $\varphi_{xy}(\tilde{\alpha}) = 1$. Полагая затем $x = 1 + \varphi_y(\tilde{\alpha})$, $y = 1 + \varphi_x(\tilde{\alpha})$, получаем в итоге набор, по которому строки $\tilde{d}_x$ и $\tilde{d}_y$ пересекаются по единицам, что противоречит условию их ортогональности. Достаточность очевидна.

Следствие 1. *Необходимым и достаточным условием ортогональности множества строк*

$$N = \bigcup_{x \in X} \{\tilde{d}_x\}$$

таблицы различимости $D(f(\tilde{x}_n), \neg)$ некоторой функции $f(\tilde{x}_n)$ является линейная разделимость функции $f(\tilde{x}_n)$ относительно множества X .

Из этого следствия и предложения 2 получаем следующие утверждения.

Лемма 1. *Справедливо неравенство*

$$\mathcal{L}(n, \neg) \geq n - t(n).$$

Лемма 2. *Если $n = 6$ или $n \geq 8$, то любая $\mathcal{L}(n, \neg)$ -достижимая функция является линейно разделимой.*

Доказательство. Пусть $f(\tilde{x}_n)$ является $\mathcal{L}(n, \neg)$ -достижимой функцией, а таблица $D(f(\tilde{x}_n), \neg)$ ее таблицей различимости. По определению, существует минимальное покрытие $\mathcal{P}(f(\tilde{x}_n))$ единиц строк этой таблицы столбцами (наборами из E_2^n), мощность которого удовлетворяет соотношению (1), а по лемме 1 и неравенству $|\mathcal{P}(f(\tilde{x}_n))| \geq n - t(n)$. Каждый набор из покрытия $\mathcal{P}(f(\tilde{x}_n))$ может быть либо единственным представителем одной и только одной строки, либо представителем сразу нескольких строк (кратко, одиночные и кратные представители). Легко видеть, что множество тех строк, которые в покрытии $\mathcal{P}(f(\tilde{x}_n))$ имеют одного

индивидуального представителя, является ортогональным множеством (обозначим его через $N^{(1)}$). Действительно, если бы какая-то пара строк из $N^{(1)}$ пересеклась по единицам, то удалив для рассматриваемых строк прежних представителей и зачислив в $\mathcal{P}(f(\tilde{x}_n))$ тот набор, по которому эти строки пересекаются, в итоге получили бы покрытие $\mathcal{P}'(f(\tilde{x}_n))$, для которого $|\mathcal{P}'(f(\tilde{x}_n))| < |\mathcal{P}(f(\tilde{x}_n))|$, что противоречит условию минимальности покрытия $\mathcal{P}(f(\tilde{x}_n))$.

Покажем, что при рассматриваемых значениях величины n , множество строк $N^{(1)}$ не пусто, т.е. $|N^{(1)}| \geq 2$. Очевидно, мы получим нижнюю границу числа одиночных представителей, если предположим, что все кратные представители являются представителями только двух строк. Тогда, если e — число одиночных представителей, а d — число кратных представителей, то согласно вышесказанному, справедливы соотношения

$$e + 2d = n, \quad e + d \geq n - t(n).$$

Следовательно, $e \geq n - 2t(n)$. Тогда при $n = 6$ и $n \geq 8$ получаем неравенство $n - 2t(n) \geq 2$.

Лемма 3. Если при $n = 6$ или $n \geq 8$ таблица различимости $D(f(\tilde{x}_n), \neg)$ некоторой функции $f(\tilde{x}_n)$, существенно зависящей от n переменных, имеет наибольшее ортогональное множество N мощности $|N| = q < n - t(n)$, то функция $f(\tilde{x}_n)$ не является $\mathcal{L}(n, \neg)$ -достижимой функцией.

Доказательство. Пусть мощность q упомянутого ортогонального множества N удовлетворяет соотношению $\lfloor n/2 \rfloor \leq q < n - t(n)$. Согласно следствию 1 функция $f(\tilde{x}_n)$ является линейно разделимой функцией относительно некоторого множества переменных X мощности q . Не нарушая общности, можно положить, что $X = \{x_1, \dots, x_q\}$, тогда

$$f(\tilde{x}_n) = \sum_{i=1}^q x_i \varphi_i + \varphi, \quad (6)$$

где сложение проводится по модулю 2.

Так как множество N является наибольшим, а следовательно, и максимальным, любая строка таблицы различимости $D(f(\tilde{x}_n), \neg)$, не содержащаяся в N , пересекается по единицам с некоторой строкой из множества N .

Покажем теперь, что любая строка из множества N пересекается по единицам с некоторой строкой, не содержащейся в N .

Пусть z есть некоторая существенная переменная функции φ_i из соотношения (6). Тогда в нормальном полиноме для функции φ_i (в множестве из $n - q$ переменных) существует конъюнкция $z\mathcal{A}$, не склеивающая ни с какой другой конъюнкцией нормального полинома для φ_i . Рассмотрим строку $\tilde{d}_z$, которая определяется вектором $\partial_z^- f(\tilde{x}_n)$. Ясно, что нормальный полином для функции $\partial_z^- f(\tilde{x}_n)$ содержит конъюнкцию $x_i\mathcal{A}$. Пусть $\tilde{\alpha}$ есть набор, обращающий конъюнкцию $\mathcal{A}$ в 1. Тогда полагая $x_i = 0$ или $x_i = 1$ в зависимости от того, содержит или не содержит нормальный полином для функции φ конъюнкцию $z\mathcal{A}$, а остальные переменные, в том числе и переменные $x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_q$, полагая равными нулю, в итоге получаем набор (размерности n), по которому пересекаются по единице строки $\tilde{d}_{x_i}$ и $\tilde{d}_z$.

Таблице различимости $D(f(\tilde{x}_n), \neg)$ поставим в соответствие простой граф (V_N, W, Γ) следующим образом. Каждой строке из множества N ставится во взаимно однозначное соответствие вершина из V_N , а каждой строке, не содержащейся в N вершина из множества W . Отображение Γ определяется тем, что паре вершин (v, w) соответствует дуга, ведущая из w в v , если отвечающие им строки пересекаются по единицам. Тогда согласно сказанному выше, для любого подмножества $A \subset W$ выполняется неравенство $\Gamma A \geq A$, где ΓA — образ множества A , т. е. выполняется условие Кенига–Холла [4]. Следовательно, существует паросочетание, отображающее множество W на множество V_N . При построении минимального покрытия будем выбирать тех представителей из N , которые являются образом при отображении W на V_N (в этом случае соответствующий набор будет представлять две строки), для остальных $q - (n - q) = 2q - n$ строк наборы, представляющие строки из N , выбираются произвольным образом. Следовательно, построенное таким образом покрытие $\mathcal{P}(f(\tilde{x}_n))$ является минимальным, поскольку $|\mathcal{P}(f(\tilde{x}_n))| = q$. Так как $q < n - t(n)$, по лемме 1 функция $f(\tilde{x}_n)$ не может быть $\mathcal{L}(n, \neg)$ -достижимой функцией.

Пусть $t(n) < q < \lfloor n/2 \rfloor$. Поменяв ролями множества W и V_N и применив к ним теорему Кенига–Холла можно построить покрытие $\mathcal{P}(f(\tilde{x}_n))$ так, что наборы, представляющие строки из ортогонального множества N , будут автоматически представлять еще q строк, не содержащихся в множестве N . Так как число представителей для оставшихся $n - 2q$ строк не превышает числа строк,

$$|\mathcal{P}(f(\tilde{x}_n))| \leq q + n - 2q = n - q < n - t(n),$$

что снова приводит к утверждению о том, что рассматриваемая функция $f(\tilde{x}_n)$ не является $\mathcal{L}(n, \neg)$ -достижимой функцией.

Пусть теперь $q \leq t(n)$ и N_1 есть удовлетворяющее условиям леммы наибольшее ортогональное множество. В соответствии с рассмотренными выше случаями при построении минимального покрытия строк таблицы различимости наборы, покрывающие строки из N_1 , можно выбрать так, что они будут представителями и других $q = |N_1|$, $q \leq t(n)$, строк, не содержащихся в N_1 . Затем среди оставшихся $n - 2q$ строк выбирается другое (если оно существует) максимальное множество N_2 . Снова можно выбрать $|N_2|$ наборов, являющихся представителями $2|N_2|$ строк и т. д. Пусть множеством N_l , $l \geq 1$, исчерпывается последовательность $N_1, N_2, \dots$ максимальных ортогональных множеств. Тогда оставшиеся

$$n - 2 \sum_{j=1}^l |N_j|$$

строк будут попарно пересекаться по единицам. Тогда, разбив произвольным образом оставшееся множество строк на пары и выбирая для каждой пары по одному представителю, можно получить покрытие для оставшихся строк, содержащее не более

$$\left\lceil \left(n - 2 \sum_{j=1}^l |N_j| \right) / 2 \right\rceil = \left\lceil n/2 - \sum_{j=1}^l |N_j| \right\rceil$$

наборов, а всего для построения минимального покрытия требуется не более

$$\left\lfloor n/2 - \sum_{j=1}^l |N_j| \right\rfloor + \sum_{j=1}^l |N_j| < \lfloor n/2 \rfloor$$

наборов. Если $n = 6$ или $n \geq 8$, то $n - t(n) > \lfloor n/2 \rfloor$, т. е. функция $f(\tilde{x}_n)$ не является $\mathcal{L}(n, \neg)$ -достижимой функцией.

Из лемм 1 и 3 и предложения 2 вытекает следующее утверждение.

Теорема 1. Если $n = 6$ или $n \geq 8$, то всякая $\mathcal{L}(n, \neg)$ -достижимая функция является линейно-разделимой функцией с наибольшей глубиной, равной $n - t(n)$.

3. Тесты для константных неисправностей

Имеется глубокая аналогия между материалом настоящего и предыдущего разделов. Поэтому однотипные доказательства, а иногда и формулировки утверждений будем опускать, уделяя больше внимания специфическим особенностям.

Соотношение (2) устанавливает взаимно однозначное соответствие между множеством констант

$$c = \{c_{i_1}, c_{i_2}, \dots, c_{i_k}\}$$

и множеством переменных

$$X = \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\},$$

которые замещаются этими константами. Поэтому в дальнейшем будем иметь дело только с множеством констант, снабженных нижними индексами, как, например, c_i или c_x .

Как и в предыдущем пункте, ради ограничения объема, рассмотрим только одиночные операции замещения переменных константами. Легко видеть, что

$$\partial_x^c f(\tilde{x}_n) = f(\tilde{x}_n) + f_x^c = x f_x^1 + (x + 1) f_x^0 + f_x^c = (x + c)(f_x^0 + f_x^1), \quad (7)$$

отсюда получаем следующее утверждение.

Утверждение 4. Любая функция $f(\tilde{x}_n)$, существенно зависящая от n переменных $x_1, \dots, x_n$, является тестируемой функцией относительно операции одиночного замещения переменной константой.

Строку таблицы различимости $D(f(\tilde{x}_n), c)$, отвечающей функции $\partial_x^c f(\tilde{x}_n)$, будем обозначать через $\tilde{d}_{c,x}$.

Из соотношения (7) также следует, что все $2n$ строк таблицы различимости образуют n ортогональных пар строк вида $(\tilde{d}_{0,x}, \tilde{d}_{1,x})$.

Пусть N есть некоторое максимальное ортогональное множество таблицы различимости $D(f(\tilde{x}_n), c)$.

Переменную $x \in \tilde{x}(N) = \{x \mid \exists c(d_{c,x} \in N)\}$ назовем парной, если $\tilde{d}_{0,x} \in N$ и $\tilde{d}_{1,x} \in N$, и одиночной, если существует одна и только одна константа c , для

которой $d_{c,x} \in N$. Эту константу назовем характеристической константой для одиночной переменной x .

Обозначим через $P(N)$ множество всех парных переменных для ортогонального множества N .

Рассмотрим произвольную пару переменных (x, y) , где $x \in P(N)$, а y — одиночная переменная с характеристической константой c . Тогда из соотношений $d_{0,x} \in N$, $d_{1,x} \in N$, $\tilde{d}_{c,y} \in N$ и $\tilde{d}_{c+1,x} \notin N$ следует, что

$$\begin{aligned} x(y+c)f_x^{0+1}f_y^{0+1} &= 0, & x(y+c+1)f_x^{0+1}f_y^{0+1} &\neq 0, \\ (x+1)(y+c)f_x^{0+1}f_y^{0+1} &= 0, & (x+1)(y+c+1)f_x^{0+1}f_y^{0+1} &\neq 0, \end{aligned} \quad (8)$$

где $f_z^{0+1} = f_z^0 + f_z^1$.

Из соотношений (8) следует, что $f_x^{0+1}f_y^{0+1} \neq 0$ и $x f_x^{0+1}f_y^{0+1} \neq 0$. Следовательно, нормальный полином для функции $x f_x^{0+1}f_y^{0+1}$ содержит непустое множество попарно отличных друг от друга конъюнкций. Поскольку умножение каждой из этих конъюнкций на множитель $y+c$ обращает всю сумму рассматриваемых конъюнкций в ноль, то любая из конъюнкций нормального полинома для функции $x f_x^{0+1}f_y^{0+1}$ содержит множитель $y+c+1$. Поскольку функция f_y^{0+1} не зависит существенно от переменной y , то множитель $y+c+1$ содержится во всех конъюнкциях нормального полинома для функции $x f_x^{0+1}$, а следовательно, и в конъюнкциях нормального полинома и для функции f_x^{0+1} . Вынося этот общий множитель за скобку, отсюда получаем, что функция f_x^{0+1} имеет вид

$$f_x^{0+1} = (y+c+1)\varphi_x \quad (9)$$

для всех $x \in P(N)$.

Переменную y , для которой $f_x^{0+1} = (y+c')\varphi_x$, $c \in \{0,1\}$, для всех $x \in P(N)$, назовем мультипликативной переменной относительно (f, N) с множителем $y+c'$. Следовательно, мы доказали следующее утверждение.

Утверждение 5. Если переменная y функции $f(\tilde{x}_n)$ является одиночной переменной с характеристической константой c для максимального ортогонального множества N , то она будет мультипликативной переменной относительно пары (f, N) функции f_x^{0+1} , $x \in P(N)$, с множителем $y+c+1$.

Имеет место и обратное утверждение. Действительно, пусть переменная z является мультипликативной переменной относительно (f, N) с множителем $z+c$. Далее, пусть множество

$$P(N) = \{y_1, y_2, \dots, y_q\}, \quad q = |P(N)|,$$

есть множество всех парных переменных функций $f(\tilde{x}_n)$. Тогда по определению

$$\begin{aligned} y_i f_{y_1}^{0+1} &= y_i(z+c)\varphi_{y_i}, \\ (1+y_i)f_{y_1}^{0+1} &= (1+y_i)(z+c)\varphi_{y_i}. \end{aligned} \quad (10)$$

Собирая в нормальном полиноме для функции $f(\tilde{x}_n)$ все члены, содержащие z ,

в силу (10) получаем, что

$$(z + c)f_z^{0+1} = (z + c) \sum_{i=1}^q y_i \varphi_{y_i},$$

$$(z + c + 1)f_z^{0+1} = (z + c + 1) \sum_{i=1}^q y_i \varphi_{y_i}.$$

Тогда

$$\begin{aligned} (z + c)f_z^{0+1}y_i f_{y_i}^{0+1} &\neq 0, & (z + c)f_z^{0+1}(y_i + 1)f_{y_i}^{0+1} &\neq 0, \\ (z + c + 1)f_z^{0+1}y_i f_{y_i}^{0+1} &= 0, & (z + c + 1)f_z^{0+1}(y_i + 1)f_{y_i}^{0+1} &= 0. \end{aligned} \quad (11)$$

Так как третье и четвертое выражения равны нулю при любом наборе $\tilde{\alpha} \in E_2^n$, отсюда следует, что строка $\tilde{d}_{c+1,z}$ ортогональна строкам $\tilde{d}_{0,y_i}$ и $\tilde{d}_{1,y_i}$, $i = 1, \dots, q$, а строка $\tilde{d}_{c,z}$ не ортогональна им, другими словами, переменная z является одиночной переменной и имеет характеристическую константу, равную $c + 1$.

Утверждение 6. Для любого максимального ортогонального множества N таблицы различимости $D(f(\tilde{x}_n), c)$ функции $f(\tilde{x}_n)$ существует не более одной одиночной переменной.

Доказательство. Предположим противное. Пусть для некоторого максимального ортогонального множества N существует пара одиночных переменных y_1 и y_2 , $y_1 \neq y_2$, с характеристическими константами c_1 и c_2 соответственно. Тогда они являются мультипликативными переменными относительно (f, N) с множителями $y_1 + c_1 + 1$ и $y_2 + c_2 + 1$. Из соотношения (9) следует, что функция f_x^{0+1} имеет вид $(y_1 + c_1 + 1)(y_2 + c_2 + 1)\psi_x$ при всех $x \in P(N)$, где $P(N)$ по-прежнему означает множество всех парных переменных для ортогонального множества N . Следовательно, строки $\tilde{d}_{c_1+1,y_1}$ и $\tilde{d}_{c_2+1,y_2}$ соответственно определяются значениями функций

$$\begin{aligned} (y_1 + c_1 + 1) \sum_{x \in P(N)} (y_2 + c_2 + 1)\psi_x &= (y_1 + c_1 + 1)(y_2 + c_2 + 1) \sum_{x \in P(N)} \psi_x, \\ (y_2 + c_2 + 1) \sum_{x \in P(N)} (y_1 + c_1 + 1)\psi_x &= (y_1 + c_1 + 1)(y_2 + c_2 + 1) \sum_{x \in P(N)} \psi_x, \end{aligned}$$

т. е. строки $\tilde{d}_{c_1+1,y_1}$ и $\tilde{d}_{c_2+1,y_2}$ совпадают, что противоречит условию их вхождения в ортогональное множество.

Аналогично следствию 1 имеет место следующее утверждение.

Утверждение 7. Необходимым и достаточным условием ортогональности множества строк N таблицы различимости $D(f(\tilde{x}_n), c)$ некоторой функции $f(\tilde{x}_n)$ является линейная разделимость функции $f(\tilde{x}_n)$ относительно некоторого множества $X \subseteq \tilde{x}_n$. Этим множеством является множество всех парных переменных.

Пусть для некоторой функции $f(\tilde{x}_n)$, существенно зависящей от n переменных, множество $N_f^{\max}$ есть наибольшее ортогональное множество таблицы различимости $D(f(\tilde{x}_n), c)$. Обозначим через $N_n^{\max}$ ортогональное множество, имеющее наибольшую мощность среди всех множеств вида $N_f^{\max}$.

Утверждение 8. *Справедливы равенства*

$$|N_n^{\max}| = \begin{cases} 2(n-t), & \text{если } 2^{t-1} + t \leq n \leq 2^t + t, \\ 2n - 2t - 1, & \text{если } n = 2^t + t + 1. \end{cases}$$

Доказательство. Пусть $N_f^{\max}$ есть максимальное ортогональное множество таблицы различимости $D(f(\tilde{x}_n), c)$ некоторой функции $f(\tilde{x}_n)$. По отношению к $N_f^{\max}$ все существенные переменные рассматриваемой функции разделим на подмножества переменных трех типов: парные, одиночные и базисные (второе подмножество может быть пустым).

Фиксируя множество из t базисных переменных, пусть это будут переменные с номерами $n-t+1, n-t+2, \dots, n$, построим функцию $f(\tilde{x}_n)$, для которой $|N_f^{\max}| = |N_n^{\max}|$. С этой целью рассмотрим множество из 2^t попарно ортогональных конъюнкций $\mathcal{A}_i, i = 1, \dots, 2^t$, одного и того же ранга t на множестве из t заданных базисных переменных. Полагая $n-t \leq 2^t$, исследуем функцию

$$g(\tilde{x}_n) = \sum_{i=1}^{n-t} x_i \mathcal{A}_i.$$

Легко видеть, что строки $\tilde{d}_{0,x_i}, \tilde{d}_{1,x_i}, i = 1, \dots, n-t$, образуют в таблице различимости $D(g(\tilde{x}_n), c)$ максимальное ортогональное множество N мощности $|N| = 2(n-t)$.

Предположим теперь, что среди $n-t$ переменных, не являющихся базисными, одна из них, скажем переменная x_{n-t} , является одиночной с характеристической константой c . Согласно утверждению (5) указанная одиночная переменная x_{n-t} является мультипликативной переменной с множителем $x_{n-t} + c + 1$, поэтому функция $g(\tilde{x}_n)$ имеет вид

$$g(\tilde{x}_n) = \sum_{i=1}^{n-t-1} x_i (x_{n-t} + c + 1) \mathcal{A}_i.$$

В этом случае наибольшее ортогональное множество $N_g^{\max}$ имеет мощность

$$2(n-t-1) + 1 = 2n - 2t - 1 < 2(n-t).$$

Другими словами, не затрагивая множества базисных переменных, мы совершили как бы перевод одной из парных переменных в одиночную, однако при этом переводе мощность наибольшего ортогонального множества понижается. Следовательно, если $n-t \leq 2^t$, то решение задачи построения функции $f(\tilde{x}_n)$, для которой $|N_f^{\max}| = |N_n^{\max}|$, необходимо рассматривать в ситуации, когда одиночные переменные отсутствуют. Тогда искомая функция $f(\tilde{x}_n)$ будет, очевидно, отвечать наименьшему значению t , удовлетворяющему неравенству

$n - t \leq 2^t$. Тогда для ближайшего значения t , предшествующего рассматриваемому минимальному значению, будем иметь уже противоположное неравенство: $n - t - 1 > 2^{t-1}$ или $n > 2^{t-1} + t$. Таким образом, если для n выполняется соотношение $2^{t-1} + t \leq n \leq 2^t + t$, то $|N_n^{\max}| = 2(n - t)$.

Рассмотрим теперь случай, когда среди небазисных переменных есть одна одиночная переменная, скажем, переменная x_{n-t} . Очевидно, в структуре соответствующей функции она расположена так, что ее перевод в разряд парных невозможен без изменения множества базисных переменных, иначе мы имели бы предыдущий случай. Ясно, что такая ситуация возможна только тогда, когда $n - t = 2^t + 1$. Учитывая, что одиночная переменная (пусть ее характеристическая константа равна c) должна быть мультипликативной, рассматриваемый случай приводит к функции

$$f(\tilde{x}_n) = (x_{n-t} + c + 1) \sum_{i=1}^{n-t-1} x_i a_i,$$

для которой наибольшее ортогональное множество имеет мощность

$$2(n - t - 1) + 1 = 2n - 2t - 1.$$

Легко видеть, что в этом случае перевод одиночной переменной в разряд парных приводит к понижению мощности наибольшего ортогонального множества. Как уже отмечалось, такой перевод требует изменения числа t базисных переменных. Действительно, наименьшее значение u , удовлетворяющее неравенству $n - u \leq 2^u$ при $n = 2^t + t + 1$ равно $t + 1$, что приводит к наибольшему ортогональному множеству мощности

$$2(n - u) = 2(n - t - 1) < 2n - 2t - 1.$$

В завершение этого раздела отметим, что в случае константных неисправностей справедлив аналог теоремы 1. Структура $\mathcal{L}(n, c)$ -достижимой функции фактически описана при доказательстве предложения 8.

4. Тесты для суперпозиций однородных двухместных функций

Пусть $f(\tilde{x}_n)$, $\tilde{x}_n = (x_1, \dots, x_n)$, — некоторая функция алгебры логики, существенно зависящая от переменных $x_1, \dots, x_n$, $J = \{J_1, \dots, J_q\}$ — семейство попарно непересекающихся подмножеств множества $\{1, \dots, n\}$, $\Phi_J = \{\varphi_{J_1}, \dots, \varphi_{J_q}\}$ — набор однотипных r_k -местных, $r_k = |J_k|$, $k = 1, \dots, q$, функций. Предметом исследования будет функция $\partial_J^\Phi f(\tilde{x}_n)$, полученная путем ∂ -операции над функцией $f(\tilde{x}_n)$, т. е.

$$\partial_J^\Phi f(\tilde{x}_n) = f(\tilde{x}_n) + f_J^\Phi(\tilde{x}_n), \quad \Phi = \Phi_J,$$

где $f_J^\Phi(\tilde{x}_n)$ есть функция, полученная из функции $f(\tilde{x}_n)$ подстановкой вместо каждой переменной x_j из множества

$$\tilde{x}_{J_k} = \bigcup_{j \in J_k} \{x_j\}$$

одной и той же функции φ_{J_k} .

Например, если $n = 6$, $J = \{\{1, 2\}, \{3, 5, 6\}\}$, а функции φ являются конъюнкциями, то для функции $f(\tilde{x}_6) = f(x_1, x_2, x_3, x_4, x_5, x_6)$ имеем

$$\partial_J^\Phi f(\tilde{x}_6) = f(\tilde{x}_6) + f(x_1 \& x_2, x_1 \& x_2, x_3 \& x_5 \& x_6, x_4, x_3 \& x_5 \& x_6, x_3 \& x_5 \& x_6).$$

Заметим, что если вместо функции $f(\tilde{x}_n)$ рассматривать ее реализацию логической схемой, например, контактной, то реализацию функции $f_J^\Phi(\tilde{x}_n)$ можно получить из схемы для $f(\tilde{x}_n)$ заменой контакта x , $x \in \tilde{x}_{J_k}$, схемой, реализующей функцию φ_{J_k} .

Теперь мы исследуем случай, когда каждое множество J_k является парой элементов, а множество J — семейством таких пар.

4.1. Тесты для конъюнкций

Пусть $f(\tilde{x}_n)$ — некоторая функция алгебры логики, (i, j) — произвольная пара из множества

$$\left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} = \bigcup_{1 \leq i < j \leq n} \{(i, j)\},$$

$F(\tilde{x}_n)$ — приведенный многочлен (полином Жегалкина) для функции $f(\tilde{x}_n)$. Тогда, используя представление

$$F(\tilde{x}_n) = x_i x_j \psi_{ij} + x_i \psi_i + x_j \psi_j + \psi, \quad (12)$$

находим, что

$$\partial_{(i,j)}^k F(\tilde{x}_n) = x_i(x_j + 1)\psi_{ij} + (x_i + 1)x_j\psi_j. \quad (13)$$

Отсюда следует, что функция $f(\tilde{x}_n)$ не является тестируемой, если $\psi_i = \psi_j \equiv 0$, т. е. если каждое вхождение переменной x_i в некоторую конъюнкцию $\mathcal{A}$ из $F(\tilde{x}_n)$ влечет за собой и вхождение в ту же конъюнкцию и переменной x_j и наоборот, каждое вхождение переменной x_j влечет за собой и вхождение в ту же конъюнкцию и переменной x_i .

Значения функций $\partial_{(i,j)}^k F(\tilde{x}_n)$, $(i, j) \in \left\{ \begin{matrix} n \\ 2 \end{matrix} \right\}$, определяют строки таблицы различимости $D(f(\tilde{x}_n), \&)$ для функции $f(\tilde{x}_n)$ (с 2^n столбцами и $n(n-1)/2$ строками). Для построения минимального покрытия необходима информация о распределении единиц рассматриваемой матрицы.

Прежде всего заметим, что функция $\partial_{(i,j)}^k F(\tilde{x}_n)$ состоит из двух взаимно ортогональных частей, поэтому для изучения множества единиц этой функции достаточно изучить одну из ее частей.

Рассмотрим функцию $x_i(x_j + 1)\psi_i$. Переменные x_i и x_j назовем определяющими переменными функции $\partial_{(i,j)}^k F(\tilde{x}_n)$. Пусть $\mathcal{A}$ есть некоторая конъюнкция приведенного многочлена для функции ψ_i , а $\mathcal{A}_1, \dots, \mathcal{A}_r$ — те части конъюнкции $\mathcal{A}$, которые содержатся в указанном многочлене (коротко, r -конъюнкции). Далее, пусть $\tilde{\alpha}_n^{(i,j)}$ есть набор наименьшего веса (с наименьшим числом компонент, равных 1), обращающий конъюнкцию $x_i \mathcal{A}$ в единицу. Тогда набор $\tilde{\alpha}_n^{(i,j)}$ обращает в единицу и все конъюнкции $\mathcal{A}_1, \dots, \mathcal{A}_r$, а при четном r обращает в единицу также и функцию $x_i(x_j + 1)\psi_i$, а в силу замечания об ортогональности частей и саму функцию $\partial_{(i,j)}^k F(\tilde{x}_n)$.

Пусть теперь $r = 0$. Отметим, что конъюнкциями с таким значением величины r являются, например, все конъюнкции минимального ранга. Легко видеть, что в этом случае определенный выше набор $\tilde{\alpha}_n^{(i,j)}$ обращает в единицу и любую функцию $\partial_{(i',j')}^k F(\tilde{x}_n)$ с ведущими переменными $x_{i'}$ и $x_{j'}$, для которых $x_{i'} \in \mathfrak{A}$, $x_{j'} \notin \mathfrak{A}$, $i = i'$, $j \neq j'$.

Таким образом, получаем, что если любая собственная часть конъюнкции $\mathfrak{A}$ приведенного мономчлена для функции $f(\tilde{x}_n)$ не содержится в нем, то существует набор $\tilde{\alpha}_n$ веса w , равный рангу конъюнкции $\mathfrak{A}$, обращающий в единицу $(n - w)w$ функций вида $\partial_{(i,j)}^k F(\tilde{x}_n)$, $x_i \in \mathfrak{A}$, $x_j \notin \mathfrak{A}$.

Таблицей пар назовем таблицу, задающую некоторое бинарное отношение ρ^2 , определенное на множестве $\{1, \dots, n\}$. Будем полагать, что это отношение является антирефлексивным и симметрическим, истинным для любой пары вида (i, j) , $i \neq j$. Следовательно, таблица пар будет заполнена всюду единицами, кроме клеток главной диагонали. Таковую таблицу будем называть полной.

Пусть $f(\tilde{x}_n)$ есть некоторая тестируемая функция, $F(\tilde{x}_n)$ — ее приведенный многочлен, $\mathfrak{A}$ — 0-конъюнкция ранга w . Тогда существует набор $\tilde{\alpha}_n$ веса w , обращающий $(n - w)w$ функций вида $\partial_{(i,j)}^k F(\tilde{x}_n)$ в единицу, в таблице пар этому набору будет отвечать заполнение $(n - w)w$ клеток единицами. Очевидно, если некоторое множество наборов является покрытием таблицы различимости, то этому множеству будет отвечать полная таблица пар.

Легко видеть, что величина $(n - w)w$ достигает максимума при $w = \lfloor n/2 \rfloor$ и минимума (что является для нас важным, поскольку рассматривается соотношение (1)) при $w = 1$ или $w = n - 1$. В последнем случае, каждый набор веса 1 (или веса $n - 1$) будет отвечать заполнению только одной строки таблицы пар, а поэтому полная таблица пар будет отвечать множеству $n - 1$ различных наборов веса 1 (соответственно, веса $n - 1$).

Таким образом, установлено, что $\mathcal{L}(n, \&)$ -достижимая функция является элементарным симметрическим полиномом $F_{k,n}(\tilde{x}_n)$ с $k = 1$ либо $k = n - 1$, где

$$F_{k,n}(\tilde{x}_n) = F_{k,n} = \sum_{1 \leq i_1 < \dots < i_k < n} x_{i_1} \dots x_{i_k}.$$

Заметим, что при $k = 1$ элементарный симметрический полином обычно называют линейной функцией.

Итак, мы доказали следующую теорему.

Теорема 2. *Справедливо равенство*

$$\mathcal{L}(n, \&) = n - 1.$$

4.2. Тесты для дизъюнкций

Пусть $f(\tilde{x}_n)$ есть некоторая функция алгебры логики, существенно зависящая от n переменных. Используя ее представление (12) для произвольной пары $(i, j) \in \{2\}^n$ для функции $\partial_{(i,j)}^\vee F(\tilde{x}_n)$ получаем выражение, аналогичное (13), именно,

$$\partial_{(i,j)}^\vee F(\tilde{x}_n) = x_i(x_j + 1)(\varphi_{ij} + \psi_i) + (x_i + 1)x_j(\psi_{ij} + \varphi_j).$$

Как и в предыдущем случае, функция $\partial_{(i,j)}^{\vee} F(\tilde{x}_n)$ состоит из двух взаимно ортогональных подфункций, а потому для нее справедливы и все рассуждения предыдущего пункта. Следовательно, $\mathcal{L}(n, \vee) = n - 1$.

Отметим, что $\mathcal{L}(n, \vee)$ -достижимыми функциями является линейная функция $f(\tilde{x}_n) = F_{1,n} = L_n$, ($\psi_{ij} = 0$, $\psi_i = \psi_j = 1$ — покрытие наборами веса 1) и симметрический полином $F_{n,n} = \bigwedge_{i=1}^n x_i$ (когда $\psi_i = \psi_j = 0$, $\psi_{ij} = F_{n-2,n-2}$ — покрытие наборами веса $n - 1$).

4.3. Тесты для сложения по модулю 2

Принципиальных отличий этого случая от предыдущих двух нет. Действительно, если $F(\tilde{x}_n)$ есть приведенный полином для функции $f(\tilde{x}_n)$, представленный в виде

$$F(\tilde{x}_n) = x_i x_j \psi_{ij} + x_i \psi_i + x_j \psi_j + \psi,$$

то

$$\partial_{(i,j)}^{\oplus} F(\tilde{x}_n) = x_i x_j (\psi_{ij} + \psi_i + \psi_j) + x_i (x_j + 1) (\psi_{ij} + \psi_j) + (x_i + 1) x_j (\psi_{ij} + \psi_i).$$

Выражение для $\partial_{(i,j)}^{\oplus} F(\tilde{x}_n)$ состоит из трех попарно ортогональных подфункций, поэтому для изучения распределения множества единиц этой функции достаточно исследовать одну из указанных ее частей. Наборы веса 1 или $n - 1$ обращают в единицу функцию $\partial_{(i,j)}^{\oplus} F(\tilde{x}_n)$ при

$$f(\tilde{x}_n) = L_n = \sum_{i=1}^n x_i$$

и при

$$f(\tilde{x}_n) = F_{n,n} = \bigwedge_{i=1}^n x_i.$$

Следовательно, $\mathcal{L}(n, \oplus) = n - 1$, а $\mathcal{L}(n, \oplus)$ -достижимыми функциями являются функции L_n и $F_{n,n}$.

Заметим, что аналогичные результаты имеют место и для остальных известных двухместных функций: импликации (прямой и обратной), антиимпликации (прямой и обратной), эквивалентности, штриха Шеффера и стрелки Пирса.

Список литературы

1. Weis C.D. Bounds on the length of terminal stuck-fault tests. *IEEE Trans. Comput.* (1972) 21, №3, 305–309.
2. Носков В. Н. О сложности тестов, контролирующих работу входов логических схем. *Матем. заметки* (1975) 18, №1, 137–150.
3. Погосян Г. Р. *О проверяющих тестах для логических схем*. Вычисл. центр АН СССР, Москва, 1982.
4. Берж К. *Теория графов и ее применения*. ИЛ, Москва, 1962.

Статья поступила 25.05.92.